IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol. 10, Issue.3, March 2022 E-ISSN: 2347-2693

A Survey on Reversible Image Steganography in Telemedicine

Bibek Ranjan Ghosh[1*], Siddhartha Banerjee[2], Subham Kr Singh[3], Shreyas Gangopadhyay[4]

[1,2,3,4]Department of Computer Science, Ramakrishna Mission Residential College, Narendrapur, Kolkata-103, India

**Corresponding author: bibekghosh2019@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v10i3.2226 | Available online at: www.ijcseonline.org

Received: 12/Feb/2022, Accepted: 13/Mar/2022, Published: 31/Mar/2022

Abstract- Electronic patient record (EPR) storage and transmission is an integral part of modern healthcare system. Steganography comes into play when the medical image becomes a potential storage of patient information. Generally steganographic techniques give higher importance to the perfect recovery of secret data than the actual reconstruction of the original image. But in medical system the actual reconstruction of the original medical image is importance as this is the primary source of disease understanding. Hence in this context reversible steganography plays an important role in telemedicine field in storing, maintenance and communication of electronic patient record within the image itself, so that where a doctor located at a geographically remote location can diagnose a patient on the basis of a medical image generated elsewhere with confidence. In this paper we have studied some elegant techniques for reversible medical image steganographic techniques and compare their performances.

Keywords- Reversible, Steganography, medical image, EPR, DICOM

I. INTRODUCTION

Steganographic techniques are used to bury data in different types of cover media like text, audio, image, video etc. Image steganography uses digital images as cover media and after embedding stego image is produced. To hide data either cover pixels are directly modified with hidden data or the image pixels are first transformed using different transform domain techniques and then the resulting coefficients are utilized to store secret information [1]. At the destination the secret data is extracted from stego image. In general, we are concerned about the perfect reconstruction of the hidden data when extracting from stego image and least interested in recovering the underlying cover image in original. If the cover image has to be perfectly reconstructed at the receiver along with secret data then it is called reversible steganography [2]. In certain applications like medical imaging this is of utmost importance [3]. In telemedicine the medical images of the patients like CT scan, MRI, X-ray etc. are transmitted over network for diagnosis elsewhere. Hence, the secrecy of the patient data has to be protected [4]. Medical images follow a specific format called Digital Imaging and Communication on Medicine (DICOM), a grayscale image having intensity levels from 0 to 4095 in 12 bit format and 0 to 65535 in 16 bit format. On the contrary, either 8-bit grayscale or 24 bit color images are used for natural images. Each cover medical image in telemedicine hides patient information i.e. electronic patient record (EPR) in DICOM image itself to produce stego image. When a diagnosis based on these images are performed by an expert doctor from a remote location the EPR has to be extracted from the stego DIACOM. The objective here is to get back the underlying DICOM in its original form so that the medical details of the DICOM is totally preserved after EPR extraction. So a reversibility of the cover is of paramount importance here. There are mainly two traits. In the former medical image is divided into two types of areas, region of non-interest (RONI) and region of interest (ROI) . The ROI are those regions of a DICOM which are necessary for disease understanding. On the other hand the areas which are less important are RONI. In general ROI areas are not used for embedding. The reversible techniques that are used for medical images are either interpolation based or difference expansion based. In interpolation based method the first original image is created by contracting the initial image to half of its original size. Then the cover image is generated by using interpolation equation from input and original image. This technique has high payload capacity but perfect reconstruction is not guaranteed. The other technique, difference expansion first create difference image from input image and a specified reference image. Then the histogram (DIH) of this difference image is shifted to create empty bins, which will be used as storage of secret data. This technique show high reversibility of cover, with additional knowledge of overflow and underflow generated by histogram shift operation. The remaining sections of this paper is arranged as stated next. Section-II discuss principle, material and methods, results found in the literature of this field, Section-III compares their performances and Section-IV conclude the study with future direction of research.

II. RELATED WORK

This section studies in details research articles published in reputed journals, related to the field under study in details.

The work by Parah S.A. et al. uses an interpolation method in medical images for reversible data hiding [5]. Initially, every pixel of the original image is up sampled into a 2x2 block, each cell containing the same pixel value. The patient information is encrypted using chaos. The EPR is embedded along with other auxiliary information like a watermark and 4x4 block checksum for authentication and localization. “Intermediate Significant Bit Substitution” (ISBS) is used for embedding to avoid common LSB attacks. Embedding is done for each block pixel other than pivot/seed pixel which is kept intact for reversibility. At the extraction step, the data is first recovered followed by the original image. The checksum is used to detect the integrity of the original images, while the watermark is used to check the integrity of the information. Average PSNR and SSIM achieved are 46.36dB and 0.9827 respectively for payload of 196608 bits or 0.75 bpb. The method performed well against many popular attacks like “salt and pepper noise” (NCC=0.9503), “Gaussian noise” (NCC=0.4979), JPEG compassion (NCC=0.5487), median (NCC=0.5439), low pass (NCC=0.5004), Weiner filter (NCC=0.5439), Sharpening (NCC=0.5053), Histogram equalization (NCC=0.5044) and rotation (NCC=0.4835). Patel et al. proposes a cloud storage-based algorithm to enhance security and management [6]. Four cloud services are required where Cloud1 stores patient id and X-ray image; Clould2 stores patient id and EPR; Cloud3 maintains patient id and key; and finally Cloud4 keeps patient id and stego image. In this method, the information is buried in the cover image by using LSB substitution. The cover image and EPR are saved in two separate clouds to enhance security. Initially is cover image is segmented into four RONI and one ROI with thresholding. A 4x4 secret key is generated which stores the initial coordinates of four RONI. After that, one of the RONIs is randomly selected and undergo pixel reduction by adjusting pixel value with the threshold in that RONI. Finally EPR is embedded in the modified RONI using LSB substitution. The stego image is stored in 4^{th} cloud. Data extraction follow the reverse path. For experiment the cover used is Shenzhen Chest X-ray database consisting of 4096x4096-X ray image of Tuberculosis. Sample EPR contains 990 characters or 7920 bits. For 2.1MB carrier and 12kB EPR PSNR achieved are 87.8 dB, 78.79 dB, 69.34 dB and 60.21 dB for 1,2,3,4 bpb embedding rate in the first RONI. Other RONIs gives similar results. 65.05dB PSNR is achieved for 256x256 DICOM color images with EPR of 18 bytes. Mantos P.L et al. proposed a reversible steganography on DICOM images [7]. At the outset, some of the rows from the top and bottom of the DICOM images are selected as RONI. The ROI embeds, the patient data consisting of sensitive medical information, hash of the data (for authentication of embedded data), hash ROI (for authentication for ROI). These three sets of data are encrypted to enhance security. This encrypted data and encryption key are embedded in the ROI. The RONI embed start row of ROI, map size which is the total number of bits altered in ROI during the embedding and the map itself in ROI. LSB matching is used for embedding. During embedding, two bits are replaced in RONI while single bit is replaced in ROI. The algorithm uses a “Pseudo Random Number Generator” (PRNG) to determine whether the bit in which is to be embedded will undergo an increment or decrement operation, keeping in mind 0 can’t be decremented and 1 can’t be incremented. In both the ROI and RONI, embedding is done by considering two halves. In ROI, the embedding occurs by considering the Sobel operator of each halves. Although the robustness of this procedure is pretty low, the imperceptivity of the algorithm is pretty high. Once tested on ten 512 × 512 & two 256 × 256 grayscale DICOM images (16bit-CTs and MRIs) maintaining a 0.25 bpb payload, the PSNR ranges 105dB to107dB while MSE ranges from 0.0830 to 0.1269. Weighted stego and Triples stego analyzer by Fridrich et al. are used to for resistance analysis [8]. Thiyagarajan P. et al. come up with a reversible method where ROI and RONI are separated using the Canny Edge Detector [9]. After that, the MD5 hash value of the ROI pixels is obtained for authentication during extraction of the embedded information. Additionally, a tree graph is generated from the hash value and the tree graph is used with 3-coloring technique to generate the key. This unique key can be generated solely from the hash value during extraction. The embedding of uses RONI region. The hash values are embedded with arithmetic progression while EPR embedding utilized 3-coloring sequence. During embedding pixels corresponding to color 1 and 2 are used. This procedure has an average PSNR value 68 dB to 74 dB for “Lungs” image for EPR length 650 to 1850 bits. The method can withstand geometric attacks like cropping, rotation and scaling. The system is very secure as the key generated using the 3 coloring of graph is almost impossible to break due to generation of huge chromatic polynomial but cover image is not fully reversible. Chandrasekaran V. et al. introduced a reversible method of data embedding with medical images with better payload capacity, least distortion [10]. So, both spatial and transform domains are used for embedding. A discrete wavelet transform (DWT) on ‘Haar’ wavelet which generate integer coefficients is used for secret data embedding, and additional reversibility information in the form of location map is stored in spatial domain with histogram modification indicating the location of the coefficients positions which are modified [11]. Binary tree is used to hold the multiple peak and zero points in difference histogram. The high and middle frequencies of DWT components are scanned in zigzag format and then the secret data in embedded. During extraction histogram recovery is applied to stego image to find the auxiliary data and then integer to integer Haar transform is used to get the image in transform domain. The proposed method is tested using R2010 sample images in MATLAB. Experimental results reveal that PSNRs are 62.56, 52.85, 50.92 and 45.85 dB at 0.1, 0.3, 0.6 and 0.8 bpb respectively for “hepatitis” image. Ni Z. et al. has come up with another reversible technique using histogram modification [12]. Initially, a histogram h is created for cover image and after scanning the histogram a set of zero point and peak point pairs are generated. “Zero point” is an intensity which no pixel have in h and "peak point" is an intensity which have maximum number of pixels. The length of hidden bits is equals the number of pixel in the peak point. Then, the image is scanned in a serial manner, and pixels that fall between (peakpoint+1) and (zero point-1), are incremented by 1. This shift the histogram by 1 place to the right leaving the bin (peakpoint+1) empty. Again image is scanned to find a pixel of peak point value. If the secret message bit is "1" then the pixel value is added with "1", and if "0" then no change is made. After embedding the new histogram has the peak point bin is reduced and (peakpoint+1) bin is filled. During extraction a pixel with peak point value indicate '0' and (peakpoint+1) indicates '1' as secret bit. After scanning the image again pixel values between (peakpoint+2) and (zero point) are reduced by 1, and original histogram is restored losslessly. This can be applied for multiple peak point and zero point pairs. Computationally simple as no transform are required. The method is tested with medical images of size 512 x 512 with payloads of 37682 bits to 184442 bits with PSNR value of 48.2 and 48.3 dB. PSNR of 48dB is claimed with average payload of 59262 bits in 512 X 512 8-bit grayscale image. Kim K.S. et al. suggested a reversible scheme with difference image histogram of sub-sampled images [13]. Initially, the cover image of size MxN is sampled with horizontal and vertical sampling factors Δu *and* Δv to create sub-sampled images, each of size M/ Δu x N/ Δv. Now, selecting one such image as reference, multiple difference images are created by subtracting the pixels of other sub-sampled images. After that difference image histogram (DIH) is created for the difference images, and then histogram shifting is done to prepare empty bins which will ultimately hold the secret bits. This shifting is done according to an embedding level L, the number of times data will be hidden in a single shifted histogram. Only central part as of DIH is used due to its high spatial correlation. After shifting mechanism with L bins are shifted to left or right. The modified DIH is verified and when a pixel of value -L or L is found, and message bit is 0 then no changes is done but if it is 1 shift of (L+1) is done if value is greater than equal to L and shift of (-L-1) is done if value if less than equal to -L .The process is repeated till L>0. At L=0, only the +L is changed which ultimately leaves out (-1) bin empty. The -1 bin in final DIH indicates there is no tampering. To avoid overflow and underflow, cyclic modular addition is used to minimize the visual disturbance as a result of pixel flipping. MSE found 0.75 when L=0 and the Δu, Δv to be 2; lower bound of PSNR is 49.38 dB. Seven 512x512 benchmark grayscale images from USC-SIPI database along with two 256 X 256, 16 bit medical DICOM images are used. The payload capacity from 6K to 210K bits is exhibited with PSNR of 50dB to 30.27 dB. For medical images PSNR lies between 31 to 35 dB with 0.25 to 0.51 bpb payload. Lee H et al. proposed a method involving expansion of DIH and error-free data hiding scheme in medical images [14]. Multiple rounds of data embedding is performed on the difference histogram to increase payload leading to overflow and underflow. For R rounds, initially *R* is subtracted from the pixel values which are more than (max pixel value-*R*) and R is added if pixel value are less than *R*. This modification is recorded on a location map and is embedded using JBIG compression. So, the original image *I* has changed into I_e (error-free image). Difference image is generated from the adjacent pixel in I_e after interpolation and subtraction. After that the DIH is used for data embedding. Now this process is iterated with R times. The paper has used MRI, CT-scans, X-ray scan images as data set and show that as R increases, the hidden data increases significantly. PSNR value after 8-bit conversion from 16 bit DICOM image exceeds 54 dB. Tai W.L. et al. stated a method based on reversible technique with DIH [15]. Initially the image is scanned in an inverse order, and pixel difference is calculated and then DIH is prepared and histogram modification is applied for data hiding. The algorithm proposes multiple passes on the histogram using various pairs of "peak point" and "zero point" for higher payload capacity. An auxiliary binary tree with L levels is used to store the multiple pairs of peak and zero points. Every tree node denotes a peak point. First the underflow and overflow situation is solved by shifting the original histogram before difference histogram is created. The DIH it shifted by 2^L to create empty bins for data embedding. The only overhead information is the level of the auxiliary binary tree for lossless data extraction. The proposed algorithm was tested multiple grayscale images of 512x512 and it was observed that while keeping L=0, the PSNR value was maintained at 48.3 dB and the bpb value was ranging between 0.1734 to 0.0375 on the data set. As L is increased payload went up to 250 kb but PSNR drops to 26.62. For payload around 33kb to 45kb the PSNR is around 48.3 dB.

III. COMPARISON

In this section we have compared the surveyed works on the basis of the following parameters and listed them in Table-1. a) Technique: The main steganography techniques and associated methods b) Encryption: The encryption techniques used for security c) Domain: Whether the technique belong to spatial, transform or both domains. d) Auxiliary information: The additional information needed for reversibility. e) Dataset: The experimental dataset f) PSNR: Peak signal to noise ratio for imperceptibility measurement g) Security Analysis: What type of security measure is taken?

Table-1: Comparison of the works under study

Sl. no	Article	Techniques	Encryption	Domain	Auxiliary information	Dataset	PSNR(dB)	Security Analysis

1	Parah S.A. et al. [5]	Interpolation of pixels, ISBS embedding	Non-linear chaos	Spatial	Watermark & block checksum for authentication	Chest X-ray, Angiography etc.	46.36 with 0.75 bpb payload	salt & peeper noise, Gaussian noise, jpeg compression, median, low pass, Weiner filtering, sharpening
2	Patel et al. [6]	Cloud based, ROI and RONI division & LSB substitution	NA	Spatial	Key value of four RONI	Shenzhen Chest X-ray database 4096x4096 X ray image Tuberculosis	87.8,78.79 , 69.34 & 60.21 for 1,2,3 & 4 bpb 12kB payload	NA
3	Mantos P.L et al [7]	ROI & RONI division & LSB substitution	Hash & public	Spatial	Hash of ROI & EPR	16 bit grayscale DICOM	105 to 107 for 0.25 bpb payload	weighted stego & triples steganalysis
4	ThiyagarajanP. et al. [9]	ROI & RONI using Canny edge detection & Arithmetic progression	MD5 hash of ROI	Spatial	Tree graph of hash with 3-coloring	DICOM images	68 to 74 for payload of 650 to 1850 bits	cropping, rotation ,scaling
5	Chandrasekaran V. et al. [10]	Integer wavelet transform(Haar & DIH shifting	NA	Hybrid	Location map & binary tree for peak and zero point	MATLAB R2010 images	62.56,52.85 ,50.92 & 45.85at 0.1,0.3,0.6 & 0.8 bpb	NA
6	Ni Z. et al. [12]	Histogram shifting	NA	Spatial	peak and zero points	512x512 DOCOM images & 1096 image CorelDraw	48.2 and 48.3 for payload of 37682 to 184442 bits	NA
7	Kim K.S. et al. [13]	Multilevel DIH shifting of sub sampled images	NA	Spatial	Overflow, underflow handling information	512x512 USC SIPI & DICOM image	50dB to 30.27 with payload 6Kb to 210Kb	NA
8	Lee H et al. [14]	Multi round DIH shifting	NA	Spatial	Location map	MRI, CT-scans, X-ray image	54	NA
9	Tai W.L. et al. [15]	DIH shifting & Overflow & underflow adjustment	NA	Spatial	Binary tree of multiple peak and zero points	512x512 grayscale image	Around 48.3 with payload 33kb to 45kb	NA

IV. CONCLUSION

In this study we had analyzed several previous works that not only deals with the storage, communication and extraction of electronic patient record in telemedicine, but also give equal importance to the perfect reconstruction of the cover image during the extraction of EPR. Some of them use spatial domain techniques and others use transform domain techniques or both. They produce quality stego images as seen from PSNR and SSIM values in experimental results, hence imperceptibility condition is met. Many of them has resistance against different steganalytic or geometric attacks, hence are very secure system. Almost all of them spare extra bits as auxiliary information for the recoverability purpose. In the future more secure transform domain technique may be used in this context.

REFERENCES

[1] B. Li, J. He, J. Huang, Y. Q. Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing., **Vol. 2, Issue.2 ,pp.142-172, 2011.**

[2] T.Lu and T. N. Vo, "Digital Media Steganography, Principles, Algorithms, and Advances", Academic Press, Egypt, **pp.189-213, 2020,** ISBN. 9780128194386

[3] G. Santhi and B. Adithya., "A Survey on Medical Image Protection using Various Steganography Techniques." , Advances in Natural and Applied Sciences,**Vol-11, Issue. 12, pp. 89-94, 2017.**

[4] S. Gulia, S. Mukherjee, T. Choudhury, "An Extensive Literature Survey on Medical Image Steganography", CSI Transactions on ICT, **Vol.4, Issue. 2, pp.293-298, 2016.**

[5] S. A. Parah, F. Ahad, J. A. Sheikh,G. M. Bhat, "Hiding Clinical Information in Medical Images: A New High Capacity and Reversible Data Hiding Technique," Journal of Biomedical Informatics , **Vol. 66 , pp.214-230, 2017.**

[6] S. K. Patel, C. Saravanan, V. K. Patel., "Cloud-Based Reversible Dynamic Secure Steganography Model for Embedding Pathological Report in Medical Images," International Journal of Computers and Applications **Vol.43, Issue.10, pp.1002-1010, 2021.**

[7] P. L. Mantos, I. Maglogiannis, "Sensitive Patient Data Hiding Using a ROI Reversible Steganography Scheme for DICOM Images.," Journal of Medical Systems **Vol.40, Issue.6, pp.1-17, 2016.**

[8] Fridrich and M. Goljan, "On Estimation of Secret Message Length In LSB Steganography in Spatial Domain," In the Proceddings SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, USA, **pp. 23-34, 2004.**

[9] P. Thiyagarajan, G. Aghila, "Reversible Dynamic Secure Steganography for Medical Image using Graph Coloring", Health Policy and Technology **Vol.2,Issue.3 , pp.151-161, 2013.**

[10] V. Chandrasekaran, P. Sevugan, "Applying Reversible Data Hiding for Medical Images in Hybrid Domain Using Haar and Modified Histogram", International Journal of Intelligent Engineering & Systems, **Vol.10, Issue.4, pp. 126-134, 2017.**

[11] W.Tai, C.Yeh, C.Chang, "Reversible Data Hiding Based on Histogram Modification of Pixel Differences", IEEE Transactions on Circuits And Systems for Video Technology, **Vol.19, Issue.6, pp. 906-910, 2009.**

[12] Z. Ni, Y.Shi, N. Ansari,W. Su, "Reversible Data Hiding", IEEE Transactions on Circuits and Systems for Video Technology **Vol.16, Issue.3, pp.354-362, 2006.**

[13] K.Kim, M.Le, H.Y.Lee,H.K..Lee, "Reversible Data Hiding Exploiting Spatial Correlation between Sub-Sampled Images", Pattern Recognition **Vol.42,Issue.11, pp. 3083-3096, 2009.**

[14] H.Y.Lee, "Reversible Data Hiding for Medical Imagery Applications to Protect Privacy", International Journal of Engineering Research and Technology **Vol.12, Issue.1, pp. 42-49, 2019.**

[15] W.L.Tai, C.M.Yeh ,C.C. Chang, "Reversible Data Hiding Based on Histogram Modification of Pixel Differences," IEEE Transactions on Circuits and Systems for Video Technology **Vol.19, Issue.6, pp. 906-910,2009.**

AUTHORS PROFILES

Bibek Ranjan Ghosh (MCA), University of North Bengal, is actively teaching as an Assistant Professor in the Department of Computer Science (CS), Ramakrishna Mission Residential College, (RKMRC) , Narendrapur Kolkata, India since 2008. He has published and presented many research articles in national and international journal and conferences including Scopus index journals. His research areas are computer vision, steganography &data science.

Dr. Siddhartha Banerjee, M.Tech (Calcutta University) Ph.D (Jadavpur University), Assistant professor, currently working as HOD in the Computer Science Department of Ramakrishna Mission Residential College, Narendrapur, Kolkata since 2008. He has published and presented many research articles in national and international journal and conferences including Scopus & SCI, WoS index journals. His research area are image processing, cryptography, VLSI & AI

Subham Kr. Singh is a under graduate student of B.Sc. honours 6th semester, in the Department of CS, RKMRC Narendrapur, Kolkata.

Shreyas Gangopadhyay is a under graduate student of B.Sc. honours, 6th semester in the Department of CS, RKMRC Narendrapur, Kolkata

