Paperless Transfer of Medical Images: Storing Patient Data in Medical Images

Helga N. Crosby, Wayne Goodridge, and Andrew Rudder, *University of The West Indies*

***Abstract*— Medical images have become an integral part of patient diagnosis in recent years. With the introduction of Health Information Management Systems (HIMS) used for the storage and sharing of patient data, as well as the use of the Picture Archiving and Communication Systems (PACS) for manipulating and storage of CT Scans, X-rays, MRIs and other medical images, the security of patient data has become a serious concern for medical professionals. The secure transfer of these images along with patient data is necessary for maintaining confidentiality as required by the Data Protection Act, 2011 in Trinidad and Tobago and similar legislation worldwide. To facilitate this secure transfer, different digital watermarking and steganography techniques have been proposed to safely hide information in these digital images. This paper focuses on the amount of data that can be embedded into typical medical images without compromising visual quality. In addition, Exploiting Modification Direction (EMD) is selected as the method of choice for hiding information in medical images and it is compared to the commonly used Least Significant Bit (LSB) method. Preliminary results show that by using EMD there little to no distortion even at the highest embedding capacity.**

***Index Terms*—Watermarking, Digital Images, Steganography, Information Hiding, Exploiting Modification Direction**

I. Introduction

In Trinidad and Tobago, medical images are used every day in the diagnosis and treatment of patients. The digital versions of these images are seen only by the medical professional performing the scan or x-ray since the infrastructure to share these images digitally has not yet been introduced throughout the hospitals and clinics island-wide. Instead, the images are printed with the patient data clearly displayed on the hard copy. Sometimes the patient data is also written on the sleeve or envelope in which the image is stored. Clearly, this process can breach the confidentiality requirement between health professionals and patients if those printed images are viewed by a third party without the patient's consent.

The introduction of an effective information hiding technique could easily facilitate the paperless transfer of medical images from the radiologist to the patient's doctor. It could also allow medical professionals to share the images for consultation with colleagues without the risk of third parties being able to link sensitive medical images to a specific patient. The concept would require each health professional to have access to an application which would enable them to retrieve the patient information.

This paper in Section II and III will explore the various information hiding techniques that currently exist and the fundamental requirements of information hiding. In Section IV the use of watermarking in digital medical images is examined. The EMD is discussed in Section V. An experiment is also presented in Section V and the results are discussed.

Manuscript received February 28, 2013.

N. Crosby was a masters' student in Computer Science at the Unversity of The West Indies, St. Augustine (e-mail: helmo.c@gmail.com).

W. Goodridge is a Lecturer in the Department of Computing and Information Technology of The University of The West Indies, St. Augustine. (e-mail: wayne.goodridge@sta.uwi.edu)).

A. Rudder is a PhD student in the Department of Computing and Information Technology of The University of The West Indies, St. Augustine. (e-mail: andrew.rudder@sta.uwi.edu).

II. Information Hiding

Information Hiding involves/includes the use of steganography and digital watermarking [1]. Watermarking is used for copyright protection, broadcast monitoring and transaction tracking. A watermarking scheme imperceptibly alters a cover object to embed a message about the cover object (e.g. owner's identifier) [2]. Some of the requirements of digital watermarking are transparency, robustness and capacity. Specifically, transparency means that the watermark embedded in the host image is imperceptible to the human eye; robustness refers to the resistance of the watermark to malicious attacks and capacity denotes the amount of data that can be hidden in the host image [3-6].

Steganography is used for secret communications. A steganographic method undetectably alters a cover object to conceal a secret message [2]. Thus, steganographic methods can hide the very presence of covert communications. Data or information hiding techniques can be carried out in three (3) domains [7] namely:

1. Spatial Domain [7] e.g. Least Significant Bit,
2. Compressed Domain [8-9] e.g. Vector Quantization (VQ) compressed images, and
3. Frequency or Transformed Domain e.g. using discrete cosine transform (DCT) [10].

Each domain has its own advantages and disadvantages in regard to hiding capacity, execution time and storage space.

DOI: 10.5176/2251-3043_3.1.234

The fundamental requirements of information hiding systems are good visual quality (i.e. image quality), high hiding capacity, robustness and steganographic security (i.e. statistically undetectable) [11].

Spatial domain methods embed the watermark by directly modifying the pixel values of the original image. These techniques include Least Significant Bit (LSB) and Exploiting Modification Direction (EMD).

In the compression domain, the secret data are embedded by the alteration of the compression code. Through the compression method, the size of the digital image data can be reduced significantly [12]. VQ is an example of a technique in the compression domain.

Transform domain methods embed the data by changing the transform domain image coefficients. Embedding a watermark in the frequency domain can provide more robust watermarking than in the spatial domain. The contourlet method is an example of this type of watermarking.

The design of data/information hiding systems presents a technical challenge. The four fundamental requirements of good visual quality, hiding capacity, robustness and steganographic security must be successfully met. The literature presents the following approaches for balancing these four requirements:

1) Increase hiding capacity or payload or embedding capacity while maintaining a good visual quality or at the cost of lower visual quality [13]. For applications requiring a high hiding capacity, this is an appropriate method.

2) Devise a robust data hiding scheme [14] that serves robust watermarking systems;

3) Enhance visual quality while keeping the same hiding capacity or at the cost of lower hiding capacity [15].

4) Devise a data hiding scheme with a high embedding efficiency [16-17]. This approach can increase the steganographic security of a data hiding scheme because it is less detectable by statistical steganalysis [18].

III. Related Literature

The popularity of digital media has resulted in the need to protect the copyright of digital distributions by hiding certain information in the original media. Thus, digital watermarking techniques have been developed for this purpose and it allows the hidden data to be retrieved to verify the integrity of the original media or to recover additional information not easily seen by the naked eye.

Digital watermarking must meet the requirements of transparency, robustness and capacity which means it must be imperceptible to the human eye, able to withstand malicious attacks and be able to effectively store as much data as possible in the watermark.

There has been great interest in the development of a benchmark to evaluate and compare the performance of various watermarking techniques; however, no benchmarking system can be relevant to all watermarking systems and applications.

Steganography, digital watermarking and cryptography are all ways of hiding information in original media but with slightly different purposes. Steganography hides the most important information. In medical imaging, for example, steganography would conceal the patient's information so as to protect the patient's privacy. On the other hand, digital watermarking hides information about the original media but the critical data would be the media itself and the watermark is designed to identify, for example, the original owner. Cryptography hides the content of the message or the signal being sent. Thus, cryptography may be applied to the patient information being hidden using a steganographic technique for additional security.

Digital Watermarking may be either robust or fragile. Robust watermarking requires that the watermark survive malicious attacks and be detected when required, whereas fragile watermarking should adjust so it is possible to identify that the original item has been illegally manipulated.

Broadcast Monitoring, Copyright Protection, Fingerprinting and Copy Control are examples of Robust Watermarking applications while Content Authentication and Integrity Verification and Medical Safety are Fragile Watermarking applications. The robust watermarking techniques generally tend to be used in the protection of distributed media while the Fragile techniques seem to have a greater application in protective services or medical applications.

A. *The Requirements of Watermarking*

The perceptual transparency of the watermark is one of the most important requirements. It refers to the fidelity of the watermarked image as compared with the un-watermarked image. While some watermarks are designed to be visible, most systems aim for invisibility.

Robustness is the second requirement of watermarking. It asserts that a watermark should be able to withstand any and all malicious attempts to remove or alter it in any way.

Private watermarking systems use informed detection which implies that the original, un-watermarked work is available during detection. Conversely, public watermarking systems used blind detection, where the original work is not available.

Where secrecy is necessary, watermark keys may be introduced for the embedding and detection process. There are three types: the private-key, the detection-key and the public-key.

Capacity is an additional property that is important to the digital watermarking process. It refers to the amount of data that can be stored in the cover data.

B. *Three Main Stages in Watermarking*

Stage 1 - Generation and Embedding

Generation of a unique and complex watermark is a critical stage of the watermarking process to ensure that the rightful owner can be identified. Watermarks can be meaningless (such as the Pseudo Random Sequence, M-Sequence or the Chaotic Sequence), or they can be meaningful (as in the Spread Spectrum Sequence, Bit Plane Decomposition or the Permutation of Watermarks).

Embedding is the combination of the watermark and the

original image. It is denoted by:

$$Y = E_k(I;W)$$

where I is the original image, W is the watermark information being embedded, k is the user's insertion key, and E represents the watermark insertion function [19], which is typically addition or multiplication. Additive watermarks are often used in spatial domain techniques while multiplicative watermarks are used in the transform domain [20].

In spatial watermarking, pseudorandom noise may be added to the intensity of the image pixels as the watermark. One of the more frequently used approaches is the Least Significant Bit (LSB) insertion. This approach can affect the robustness as well as the invisibility as the watermark is seen as noise added to the signal, which is the cover data when transmitted.

Transform domain watermarks such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fractal Transform hide watermarking signals in the transform coefficients. The embedding process adds the watermark signal as Gaussian white noise into the medium and high frequency components of the original image, which leaves the lowest frequency component intact for the fidelity of the system.

Each of these watermarking techniques has its advantages and disadvantages. The advantage of the spatial domain techniques is that they are fast and easy to implement; however, they are at a disadvantage when facing potential attacks. On the other hand, transform domain techniques have a high computational cost, but they are robust and of good quality.

Stage 2 - Distribution and Possible Attacks

After embedding the watermarks in the cover image, the watermarked image is distributed. The watermarking channel through which it is distributed includes the possible attacks on the watermarks.

Possible attacks include Simple Attacks which may result from the normal manipulations of an image; Removal Attacks which attempt to separate the watermark from the cover image and then delete it; Oracle attacks which focus on the security issues; Ambiguity attacks which aim to cause confusion by embedding a fake watermark signal and Geometrical attacks which seek to make detection impossible by destroying the synchronisation of detection.

Stage 3 – Detection

Depending on the way in which the watermark is inserted into the cover image, as well as the nature of the watermarking algorithm, there can be distinct approaches to the detection method. Many detection methods use the exact inverse process of embedding to get the watermarks. Where pseudorandom noise is inserted, the correlation can be computed to determine the existence of a watermark in the image. The detection can be represented as follows:

$$W = D(I, Y)_k$$

where I is the original image (not required for oblivious techniques), Y is a possibly corrupted representation of the watermark extraction/detection function, watermarked image k is the extraction key, D and W represent the extracted watermark information [19].

C. Information Hiding and Cryptography

Information Hiding is a blanket term that encompasses digital watermarking and Steganography. As mentioned before, the approach of each of these subsets is slightly different. While digital watermarking seeks to transmit the original cover image with identifying information hidden in that image, steganography attempts to transmit a hidden message which is concealed in the cover image. Thus, steganography mandates imperceptibility while this is optional for digital watermarking.

Cryptography, unlike information hiding, tries to hide the content of the information being transmitted, concealing the subject matter itself. While information hiding and cryptography are quite different, information hiding techniques borrow many ideas from cryptography in practice.

IV. Watermarking in Medical Imaging

Watermarking can be used to authenticate medical images. For example, if a medical image is illegally obtained and the content is changed, then the incorrect diagnosis can be deduced. By putting a watermark in the medical image and authenticating this watermark before usage could prevent this threat [21]. However, if the watermark can be easily detected then it can be removed or even replaced [22-23]. When watermarking is used for authenticating medical images public key cryptography is typically used where a digital signature is computed over the whole image or over some specific part of the image. This digital signature is then used to ensure that the security principles of integrity and non-repudiation are maintained.

Another way watermarking is used in medical images is to hide confidential patient data in images [24-27]. The main drawback of this application of watermarking is the fact that the size of the message that can be embedded in a medical image without degrading the quality is a critical factor and depends heavily on the watermarking technique used. Of course, another obvious drawback is the fact that all medical cases may not involve the use of medical images.

In this paper we will focus on only the spatial domain and embedding additional information into medical images in this domain requires extreme care because the medical image quality must be maintained. LSB based watermarking is straightforward and previously used in [28, 29]. Although LSB based approaches have high embedding capacities the main drawback is that these approaches are not secured because of ease of deduction of the presence of a watermark [30].

V. The Proposed Solution

The chosen steganography technique for this application is a variable bit embedding strategy, Exploiting Modification Direction as proposed in [31].

This technique allows for a higher capacity of data to be

embedded into the grayscale image with minimal degradation of the image quality. In medical images, maintaining the image quality is critical to ensuring accurate diagnosis. Therefore, this technique is good for achieving this goal.

This scheme embeds a secret message M into a grayscale cover image X facilitated by an extraction function F which is used to create a mapping matrix S sized 256x256:

$F(x_i,x_{i+1}) = \lceil (s-1) \times x_i + s \times x_{i+1} \rceil \bmod s^2$

Where $s \geq 2$ and $0 \leq x_i, x_{i+1} \leq 255$

$\therefore$ F generates a number belonging to the set $\{0, 1, ., s^2 - 1\}$

The embedding procedure is as follows:

Step 1: Generate the matrix S sized 256x256 by using the extraction function, F, defined above.

Step 2: Compute $k = \lfloor log_2 s^2 \rfloor$, $r = \lfloor s/2 \rfloor$

Step 3: Set $i = 1$

Step 4: Read the next k secret bits $(m_1 m_2 \ldots m_k)$ from M and convert them into the decimal number d.

Step 5: Read the next cover pixel pair (x_i, x_{i+1}) from X according to the user-defined pairing rule.

Step 6: If $d = S[x_i]\,[x_{i+1}]$, then the grayscale stego pair is attained by $(y_i, y_{i+1}) = (x_i, x_{i+1})$.

Otherwise, search from the searching square:

$W_{(2\times r+1)\times(2\times r+1)}(s,\ (x_i, x_{i+1}),\ r)$ to find out the element $S[p][q] = d$ with the minimum distortion embedding (MDE) which is calculated as: $d_{min} = min_{j=a,t,w}\{|x_i - x_j| + |x_{i+1} - y_j|\}$

Then, the grayscale stego pixel pair is achieved by $(y_i, y_{i+1}) = (p, q)$

Step 7: Set $i = i + 2$

Step 8: Repeat Step 4 through Step 7 until all secret bits are embedded.

The extraction phase requires the authorised receiver to know the value of s so that $k = \lfloor log_2 s^2 \rfloor$ may be calculated. For each stego pixel pair (y_i, y_{i+1}) in the stego image Y, the embedded secret number is extracted using $d = F(y_i, y_{i+1})$. d is then converted back to k original secret bits $(m_1 m_2 \ldots m_k)$ and appended to the message M. This process is repeated until all the secret number ds are extracted and the original secret message, M, is retrieved.

A. The Prototype

A prototype coded in MS Visual C# is built and used by radiologists to save reports and patient information within a medical image. As shown in Figure 1, the original image is loaded into the area on the top left of the screen for the radiologist to review. The radiologist then enters the relevant patient information and the report of his/her findings and uses the 'Embed Text' feature to embed the text into the image, thus creating a stego image which is then displayed on the right. The stego image can then be saved and later retrieved so the text could be extracted.

B. Experiment and Results

An Intel Core i3-2310 CPU running at 2.1 GHz with 4 GB RAM was used to perform testing with eleven (11) different images as shown in Figure 2.

The images used for the experiment are varied in size; however, they were all square for the purpose of this study only. Figure 2 shows the 11 images that were used but in the real world, medical images would vary in size and are often rectangular.

The indicator used to determine the quality of the stego image when compared with the original cover image was the Peak Signal to Noise Ratio (PSNR). The hiding capacity (shown in Table 1) was obtained by calculating the bits per pixel (BPP) by taking the total number of bits embedded in a given stego image and dividing it by the number of pixels in the stego image itself.

With each method, the PSNR values are compared based on the Embedded Bit Per Pixel (shown as BPP in Table 2 above). The value n represents the size of the search area for the grid used by the algorithm – for example, if n = 4, then the search area is 4 x 4 = 16. From the data, it is clear that if we use this comparison alone, LSB Replacement would appear to be the better method for BPP at 1 or 2; however, as the embedded bits per pixel increased, the signal is considerably degraded when using LSB Replacement whereas it improves with EMD.

It must be noted that if this table was to be taken as the only evidence for embedding data in medical images, the concept would immediately be dismissed since the PSNR is low for all values of BPP between one (1) and four (4). Therefore, we must look at the other factors.

The pictures in Figure 3 demonstrate the distortion that is seen in both methods; notice that as the BPP increases, LSB Replacement degrades to a completely unusable image while EMD allows for the embedding of more data with little to no distortion.

Figure 3 shows the watermarked images with the LSB Replacement applied to the left column and EMD to the right.

The graph in figure 4 below shows the progression of the images above by comparing the Peak Signal to Noise Ratio (PSNR) for LSB Replacement against Exploiting Modification Direction (EMD) for embedded bits per pixel from 1 to 8.

PSNR for LSB Replacement is better than EMD for embedding one (1) to three (3) bits per pixel; however, a PSNR of 50 and lower could result in some distortion of the image which may result in a misdiagnosis.

Before making a confirmed decision, however, consider figure 5, which is a graph of PSNR for another image which seems to have a larger region of interest. In this case, the graphs of LSB and EMD almost mirror each other but the result is the same: as BPP increases, the PSNR for EMD increases while the PSNR for LSB Replacement decreases.

The images in Figure 6 show that there is no distortion easily detected by the human eye for EMD but from BPP = 2, LSB Replacement shows signs of distortion.

All the other images used in these experiments display similar characteristics with regard to the relationship between PSNR and BPP for each of the methods used.

The two tables below demonstrate this relationship in the data presented. Table 3 displays the PSNR against BPP for each of the images using LSB Replacement as well as the overall average for the method. Table 4 shows the PSNR against BPP for each of the images using EMD along with the averages.

The averages, which have been plotted in Figure 7 below, reflect the same results that were shown in the examples above which clearly depicts EMD as being the better method for embedding data in the medical images.

For each image, the result is the same regardless of size or content. While some of the graphs may not have shown a constant increase as seen in the graph of averages; as the amount of data embedded increased, the conclusion is the same: EMD is the safer method for embedding data in medical images since there is little to no distortion even at the highest embedding capacity.

Figures 8 to 14 are the graphs for the other images used in this study and they show further confirmation of the hypothesis that EMD is the better method for this purpose.

VI. Future Work

The application outlined above shows a very basic process for loading an original image and embedding text into a medical picture so that it may be shared with other professionals while protecting the patient's confidentiality.

In a revision of the application, the patient information would be automatically populated from the PACS system and only the report would have to be typed by the radiologist.

Additionally, the algorithm would be refined so the text would only be embedded in the Region of Non-Interest (RONI) of the image. That is, the algorithm will systematically detect an area of the image that contains no medical data so it would be further guaranteed that the embedded data could have no deleterious effect on the accurate diagnosis of the patient.

The application will also be further developed so the physician would be able to add his or her own notes to the image in the event that additional consultation is required.

VII. Conclusion

The use of medical images in patient diagnosis continues to advance, as it remains critical to accurate patient diagnosis. While PACS has been successfully implemented at one of the Regional Health Authorities in Trinidad and Tobago, currently it is only available to the patients who visit the facilities on the eastern end of Trinidad. Patients outside of that region still receive printed X-rays, CT Scans and MRIs to take to their doctor at the risk of revealing their information to unintended third parties.

The system proposed in this paper is a secure alternative for the patients visiting the other medical institutions in the island.

This study sought to achieve the following objectives:

1. *To build a system for encoding of patient information in medical images.* The application created embeds the patient information in the medical images through steganography by utilising the Exploiting Modification Direction (EMD) method.

2. *To examine the applicability and security of embedding data in digital medical images.* This study has provided evidence to support the feasibility of embedding data in medical images without distorting the image so patient diagnosis will be unaffected. The information embedded would be secure since the access to the application would be provided only to authorised medical personnel.

3. *To apply the concept of steganography to digital medical images*. Exploiting Modification Direction was successfully used to embed the patient data in the medical images.

4. *To provide a secure environment that allows medical staff to embed patient information into digital images.* The application created may be integrated into a larger HIMS or simply be revised to require a password to gain access. The system proposed protects the patient's data since a third party would not be able to identify the existence of data in the stego image nor would they have access to the code that would allow them to extract that information.

5. *To create a user-friendly interface for use by medical staff to safely encode patient information within medical images.* The interface is easy to use so medical personnel would not have to go through a lengthy process that would delay patient treatment.

Thus, until PACS can be deployed throughout the system with the features of network access as well as remote access to authorised users, this proposed application could serve as a confidential alternative for practitioners to view medical images securely, to transmit confidential patient information for consultation with peers and to record additional information to track patient progress.

References

1. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). "Information hiding – A survey." *Proceedings of the IEEE*, 87(7), 1062-1078
2. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2007). "Digital watermarking and steganography." Morgan Kaufmann. ISBN 978-0-12-372585-1.
3. S. Erküçük, S. Krishnan, and M. Zeytinoğlu, "A robust audio watermark representation based on linear chirps," *IEEE Transactions on Multimedia*, vol. 8, no. 5, Article ID 1703507, pp. 925-936, 2006.
4. F. Chuchong, D. Kundur, and R.H. Kwong, "Analysis and design of secure watermark-based authentication systems," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 43-55, 2006.
5. Y. Feng, N. H. Ling, G. Lin, W. Zhe, and W.J. Zhang, "Transmitter identification with watermark signal in DVB-H signal frequency network," *IEEE Transactions on Broadcasting*, vol. 55, no. 3, Article ID 5170023, pp. 663-667, 2009.
6. A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences, (HICSS '02)*, pp. 2043-2048, Big Island, Hawaii, USA, January 2002.
7. Lu-Ting Ko, Jwu-E. Chen, Yaw-Shih Shieh, His-Chin Hsin & Tze-Yun Sung, "Nested Quantization Index Modulation for Reversible Watermarking and Its Application to Healthcare Information Management Systems," *Computational and Mathematical Methods in Medicine*, Volume 2012, Article ID 839161, 8 pages.

8. The Duc Kieu, Chin-Chen Chang, "A steganographic scheme by fully exploiting modification directions," *Expert Systems with Applications* 38 (2011) 10648-10657 www.elsevier.com/locate/eswa
9. F. Rahimi, H. Rabbani, "A dual adaptive watermarking scheme in contourlet domain for DICOM images," *Biomedical Engineering OnLine* 2011,10:53, http://www.biomedicalengineeringonline.com/content/10/1/53
10. Lee, S., Yoo, C. D., & Kalker, T. (2007). "Reversible image watermarking based on integer-to-integer wavelet transform." *IEEE Transactions on Information Forensics and Security*. 2(3), 321-330.
11. Langelaar, G. C., Setyawan, L., & Lagendijk, R. L. (2000). "Watermarking digital image and video data: a state-of-the-art overview." *IEEE Signal Processing Magazine*, 17(5), 20-46.
12. Zhi-Hui Wang, Chin-Chen Chang & Pei-Yu Tsai, "Hiding Secret Data in an Image Using Codeword Imitation," *Journal of Information Processing Systems*, vol. 6, no. 4, Dec 2010
13. T. H. Lan & A. H. Tewfik, "A novel high capacity data-embedding system." *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2431-2440, 2006.
14. Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun & X. Lin (2008). "Robust lossless image data hiding designed for semi-fragile image authentication." *IEEE Transactions on Circuits and Systems for Video Technology*, 18(4), 497-509.
15. Z. Ni, Y. Shi, N. Ansari & W. Su (2006). "Reversible data hiding", *IEEE Transactions on Circuits and Systems for Video Technology*, 16(3), 354-362.
16. J. Fridrich, M. Goljian & D. Soukal (2006). "Wet paper codes with improved embedding efficiency." *IEEE Transactions on Information Forensics and Security*, 1(1), 102-110.
17. A. Westfield (2001). "F5-A steganographic algorithm." In *Proceedings of 4th International Workshop on Information Hiding*. LNCS (Vol. 2137, pp. 289-302). Springer
18. J. Fridrich, P. Lisonek, & D. Soukal (2007). "On steganographic embedding efficiency." In *Proceedings of 8th International workshop on Information Hiding*. LNCS (vol. 4437, pp. 282-296). Springer.
19. Chandramouli, R. and N. Memon. "How many pixels to watermark?" in *Information Technology: Coding and Computing*, 2000. Proceedings. International Conference on. 2000.
20. Bami, M., et al., "Watermark embedding: hiding a signal within a cover image." *Communications Magazine*, IEEE, 2001. 39(8): p. 102-108.
21. G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevance of Watermarking in Medical Imaging", in *Proceedings of the IEEE EMBS Conf. on International Journal of Computer Applications and Technology* (2278 - 8298), Volume 1 – Issue 1, 2012, 30-39
22. Zain, J.M.; Fauzi, A.R.M., "Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR)", *29th Annual International Conference of the IEEE on Engineering in Medicine and Biology Society*, EMBS 2007. pp. 5661-5664, 2007.
23. Velumani, R.; Seenivasagam, V., "A reversible blind medical image watermarking scheme for patient identification, improved telediagnosis and tamper detection with a facial image watermark", *IEEE International Conference on Computational Intelligence and Computing Research* (ICCIC), pp. 1-8, 2010
24. R. Acharya, U.C. Niranjan, S.S. Iyengar, N. Kannathal, L.C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," *Computer Methods and Programs in Biomedicine*, vol. 76, pp.13-19, 2004.
25. J. Nayak, P.S. Bhat, M.S. Kumar, R. Acharya, "Reliable transmission and storage of medical images with patient information using error control codes," in *Proc. IEEE INDICON*, 2004, pp.147-150.
26. Y. Srinivasan, B. Nutter, S. Mitra, B. Phillips, D. Ferris, "Secure transmission of medical records using high capacity steganography," in *Proc. 17th IEEE Symposium on Computer Based Medical Systems*, 2004, p.122-127.
27. D. Anand, U.C. Niranjan, "Watermarking Medical Images with Patient Information," in *Proc. Int. Conf. IEEE-EMBS*, 1998, pp. 703–706.
28. P. Koushik, G. Goutam and M. Bhattacharya, "A Comparative Study between LSB and Modified Bit Replacement (MBR) Watermarking Technique in Spatial Domain for Biomedical Image Security", *International Journal of Computer Applications Technology and Research*, vol. 1, No. 1, 2012, pp. 30-39.
29. M.A Hajjaji, A. Mtibaa and E. Bourennane, "A Watermarking of Medical Image: Method Based "LSB"", *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, No. 12, 2011, ISSN 2079-8407.
30. Ramani K.; Prasad E.V, Varadarajan S.; Subramanyam A,"A Watermarking Scheme for Information Hiding and Communications", *16th International Conference*, 14 pp: 58 – 64.
31. The Duc Kieu & Chin-Chen Chang, "A Reversible Watermarking Scheme with High Payload and Good Visual Quality for Watermarked Images," *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 11, November 2011.
32. Mielikainen, J. (2006). "LSB matching revisited." *IEEE Signal Processing Letters*, 13(5), 285-287.
33. Chang, C. C., Kieu, T. D., & Chou, Y. C. (2009a). "Reversible information hiding for VQ indices based on locally adaptive coding." *Journal of Visual Communication and Image Representation*, 20(1), 57-64.
34. Chang, C. C., Kieu, T. D., & Wu, W. C. (2009). "A lossless data embedding technique by joint neighbouring coding." *Pattern Recognition.* 42(7), 1597-1603.
35. Chang, C. C., Tai, W. L., & Lin, C. C. (2006). "A reversible data hiding scheme based on side match vector quantization." *IEEE Transactions on Circuits and Systems for Video Technology*, 16(10), 1301-1308.
36. X. P. Zhang & S. Z. Wang, "Efficient Steganographic embedding by exploiting modification direction", *IEEE Communications Letters*, vol. 10, no. 11, pp. 1-3, 2006
37. C. C. Chang & C. Y. Lin, "Reversible steganography for VQ-compressed images using side matching and relocation", *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 4, pp. 493-501, 2006.
38. Y. T. Wu & Y. S. Frank, "Digital watermarking based on chaotic map and reference register", *Pattern Recognition*, vol. 40, no. 12, pp. 3753-3763, 2007.
39. C.C. Chen & D. S. Kao, "DCT-based zero replacement reversible image watermarking approach", *International Journal of Innovative Computing, Information and Control*, vol. 4, no. 11, pp. 3027-3036, 2008.
40. H-.M. Chao, C-.M. Hsu, S-.G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Trans. on Information Technology in Biomedicine*, vol.6, n°1, pp.46-53, 2002.

Helga N. Crosby was born in Cocorite, Trinidad and Tobago in June 1976. She is currently reading for a Master of Computer Science at the University of the West Indies, St. Augustine, Trinidad & Tobago with a completion date of June 2013. Crosby completed her BSc. (Hons) Computer Science and Management in June 2003 and went on to work in the industry both in Trinidad and Tobago and in England, U.K. She spent some time as a Teaching Assistant in the Department of Mathematics and Computer Science at the University of the West Indies before returning to the corporate world in the sale of Information and Communication Technology. She currently lives and works in Ontario, Canada with her partner while continuing to work in the field of Information Technology.

Wayne Goodridge is a Lecturer in the Department of Computing and Information Technology, The University of the West Indies, St. Augustine. He did his PhD at Dalhousie University and his research interest includes computer communications and security.

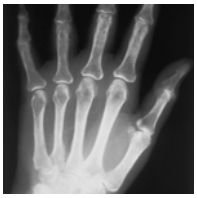
Andrew Rudder is an Assistant Lecturer in the Department of Computing and Information Technology, The University of the West Indies, St. Augustine. His area of research is Digital watermarking and Steganography.

Fig 1 - The embedded text is Extracted and displayed in the textbox on the right

a. brokenArm 1

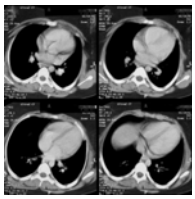
b. brokenHand2

c. chestXray 3

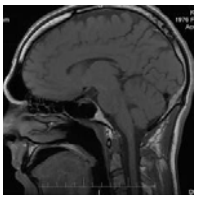


d. brokenHand4

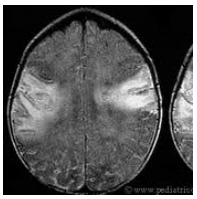
e. neck5



f. CTScan6

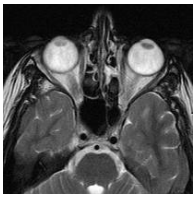


g. brainScan7



h. brain8

i. chestScan 9



j. headScan10

k. legScan11

Fig 2 – Eleven images used for testing

	Width	*Height*	*Embedding Capacity*
BrokenArm1	300	300	90000
BrokenHand2	256	256	65536
ChestXray3	480	480	230400
BrokenHand4	334	334	111556
Neck5	392	392	153664
CTScan6	402	402	161604
BrainScan7	224	224	50176
brain8	172	172	29584
chestScan9	194	194	37636
HeadScan10	206	206	42436
LegScan11	200	200	40000

Table 1 – Size and Capacity of Images

Cover Image	*LSB Replacement*				*EMD (n=2)*	*EMD (n=4)*	*EMD (n=6)*	*EMD (n=8)*
	BPP=1	*BPP=2*	*BPP=3*	*BPP=4*	*BPP=1*	*BPP=2*	*BPP=3*	*BPP=4*
BrokenArm1	51.18	43.20	36.29	29.76	19.65	25.22	32.13	38.40
BrokenHand2	51.15	43.60	36.85	30.41	23.95	30.09	37.36	70.08
ChestXray3	51.15	44.18	38.65	32.77	32.64	38.38	43.16	53.50
BrokenHand4	51.15	44.15	37.79	31.76	28.96	34.32	40.90	50.41
Neck5	51.14	43.93	37.39	32.52	52.11	57.14	63.19	69.29
CTScan6	51.15	43.79	37.32	31.09	20.54	26.06	31.70	38.27
BrainScan7	51.15	44.15	38.00	32.22	26.82	32.36	39.99	69.25
brain8	51.12	44.09	38.04	31.57	23.06	27.80	31.69	41.69
chestScan9	51.16	44.12	37.95	31.80	26.06	31.43	37.29	45.73
HeadScan10	51.13	44.10	37.81	32.12	26.62	32.11	37.81	41.49
LegScan11	51.10	44.68	38.17	32.27	29.37	35.57	45.93	46.00
Average	***51.14***	***44.00***	***37.66***	***31.66***	***28.16***	***33.68***	***40.10***	***51.28***

Table 2 – LSB vs. EMD for BPP = 1 to 4

LSB Replacement

BPP = 1, PSNR = 51.18 dB

BPP = 2, PSNR = 43.20 dB

BPP = 3, PSNR = 36.29 dB

EMD

BPP = 1, PSNR = 19.65 dB

BPP = 2, PSNR = 25.22 dB

BPP = 3, PSNR = 32.13

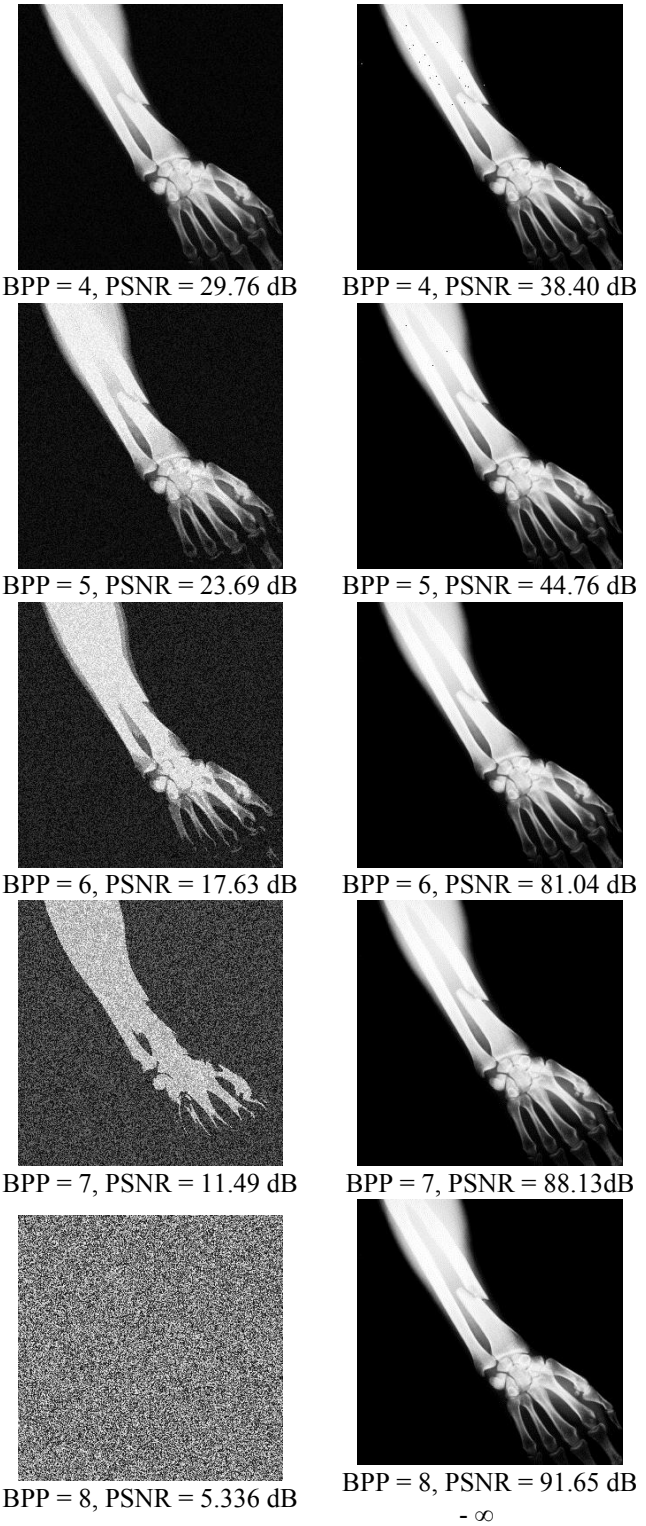


Fig 3 – Comparison of LSB Replacement and EMD

LSB Replacement

Bits per pixel	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
BrokenArm1	51.18	43.20	36.29	29.76	23.69	17.63	11.49	5.34
BrokenHand2	51.15	43.60	36.85	30.41	24.18	18.05	11.96	5.82
ChestXray3	51.15	44.18	38.65	32.77	26.00	20.01	14.45	8.48
BrokenHand4	51.15	44.15	37.79	31.76	25.99	20.42	13.90	7.49
Neck5	51.14	43.93	37.39	32.52	26.45	19.54	12.87	6.43
CTScan6	51.15	43.79	37.32	31.09	24.78	18.96	12.86	6.89
BrainScan7	51.15	44.15	38.00	32.22	25.92	19.12	14.28	7.41
brain8	51.12	44.09	38.04	31.57	25.28	19.10	12.92	7.29
chestScan9	51.16	44.12	37.95	31.80	25.75	19.76	13.85	9.36
HeadScan10	51.13	44.10	37.81	32.12	25.96	19.77	13.66	7.38
LegScan11	51.10	44.68	38.17	32.27	25.17	18.68	12.21	6.35
Average	***51.14***	***44.00***	***37.66***	***31.66***	***25.38***	***19.19***	***13.13***	***7.11***

Table 3 – LSB Replacement – PSNR x BPP

EMD

Value of n	*2*	*4*	*6*	*8*	*10*	*12*	*14*	*16*
Bits per pixel	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
BrokenArm1	19.65	25.22	32.13	38.40	44.76	81.04	88.13	91.65
BrokenHand2	23.95	30.09	37.36	70.08	48.15	48.16	88.51	96.29
ChestXray3	32.64	38.38	43.16	53.50	75.30	80.68	86.98	94.76
BrokenHand4	28.96	34.32	40.90	50.41	50.46	50.47	88.19	93.83
Neck5	52.11	57.14	63.19	69.29	75.16	81.02	85.52	92.21
CTScan6	20.54	26.06	31.70	38.27	45.09	47.31	89.42	92.43
BrainScan7	26.82	32.36	39.99	69.25	46.99	81.71	90.36	89.11
brain8	23.06	27.80	31.69	41.69	44.70	80.05	85.85	92.84
chestScan9	26.06	31.43	37.29	45.73	45.75	81.84	87.86	93.88
HeadScan10	26.62	32.11	37.81	41.49	75.89	79.93	85.95	89.63
LegScan11	29.37	35.57	45.93	46.00	75.76	83.01	87.16	94.14
Average	***28.16***	***33.68***	***40.10***	***51.28***	***57.09***	***72.29***	***87.63***	***92.80***

Table 4 – EMD – PSNR x BPP

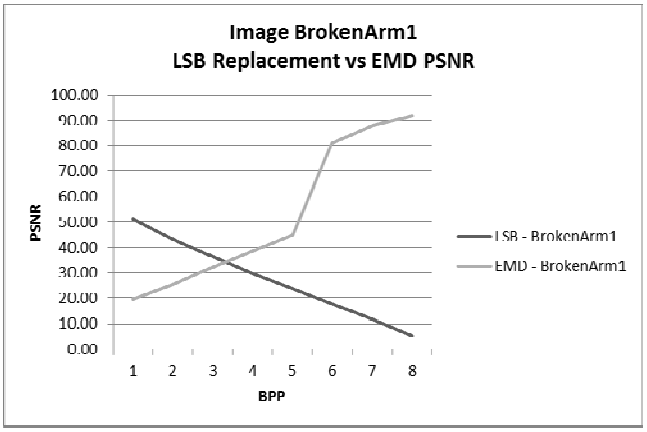


Fig 4 – Graph for Image 1 – LSB vs EMD

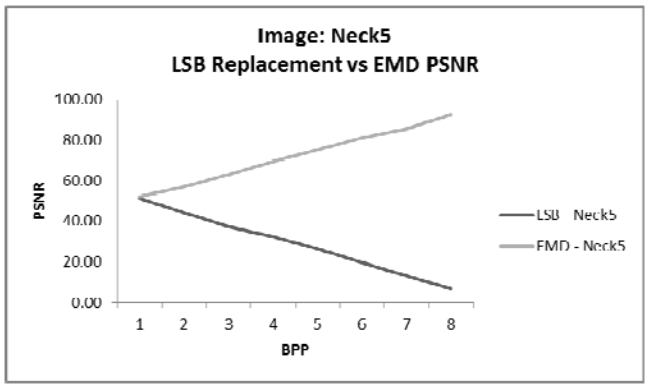
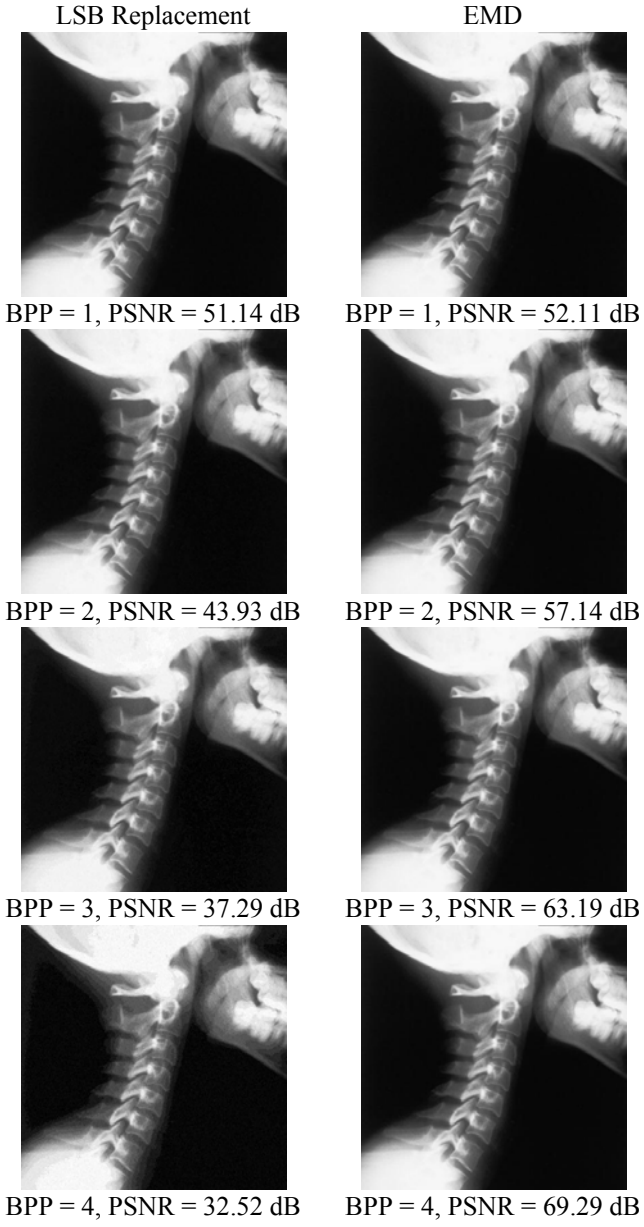


Fig 5 – Graph for Image 5 – LSB vs. EMD



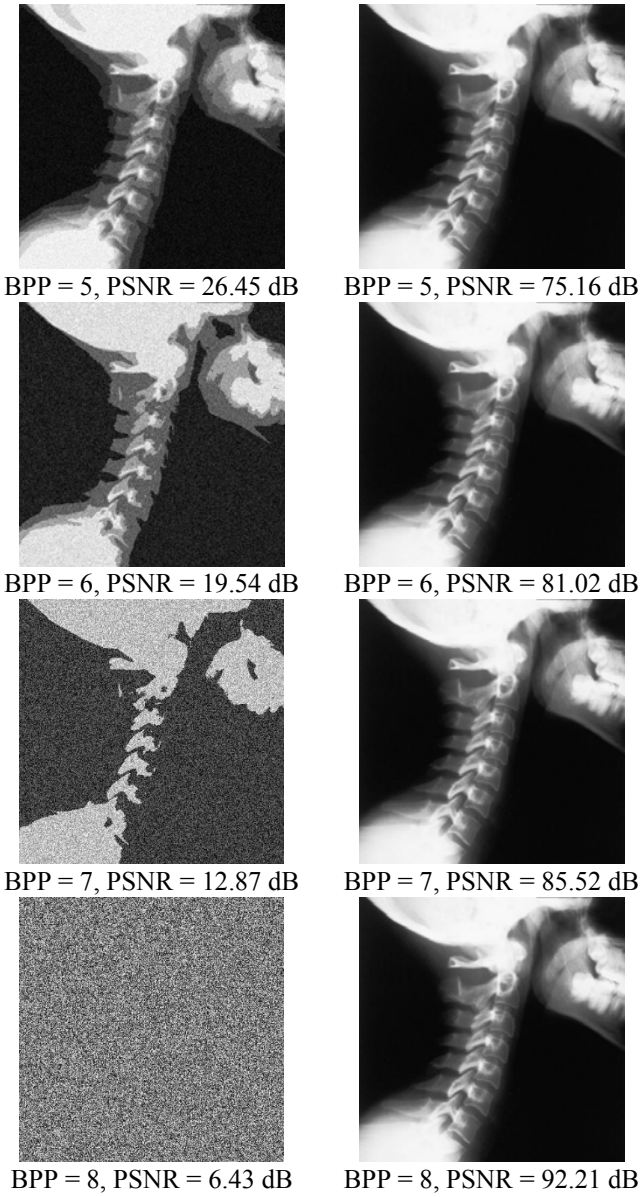


Fig 6 – Neck5 Progression for LSB vs. EMD

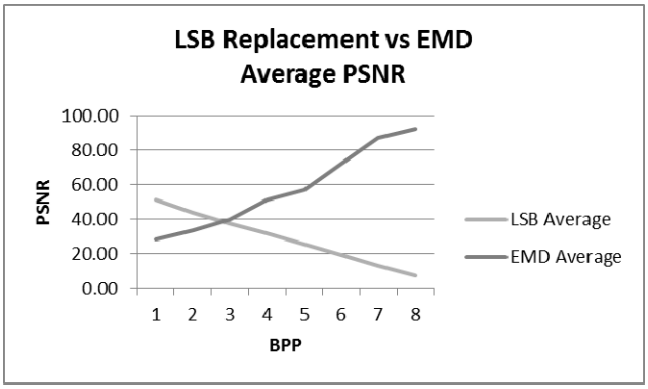


Fig 7 – LSB Replacement vs. EMD – Average PSNR

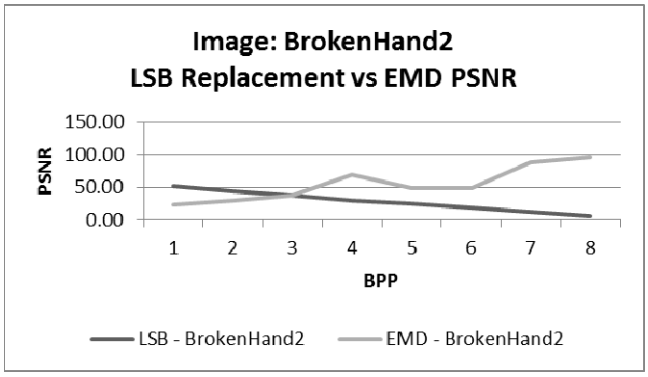


Fig 8 – BrokenHand2 - PSNR

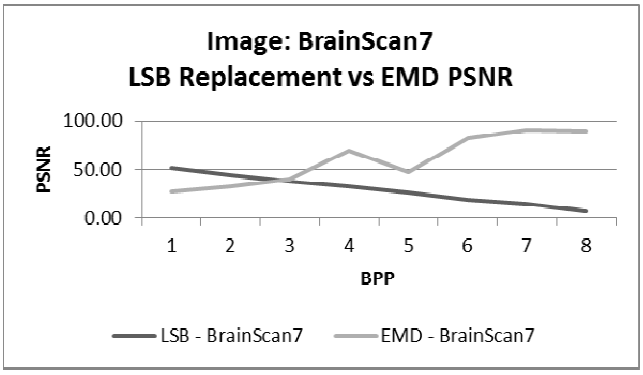


Fig 12 – BrainScan7 - PSNR

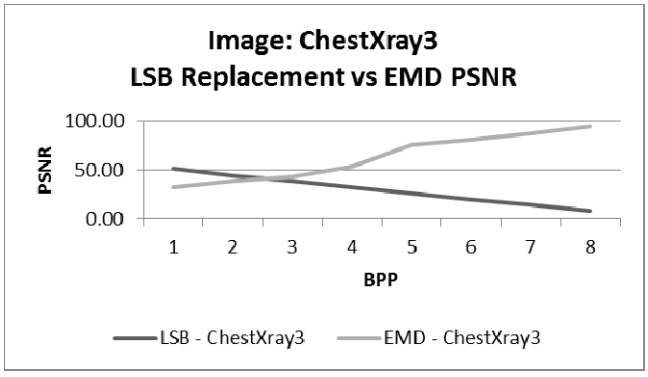


Fig 9 – ChestXray3 - PSNR

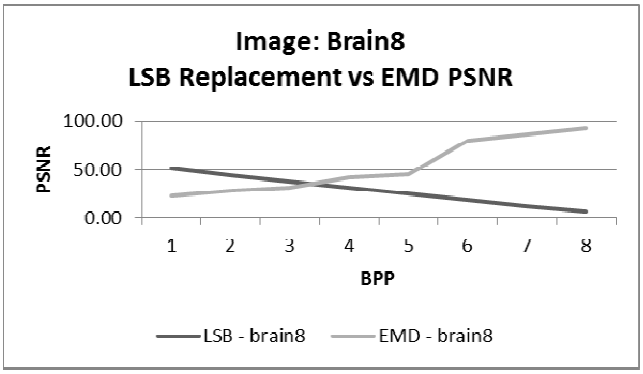


Fig 13 – Brain8 - PSNR

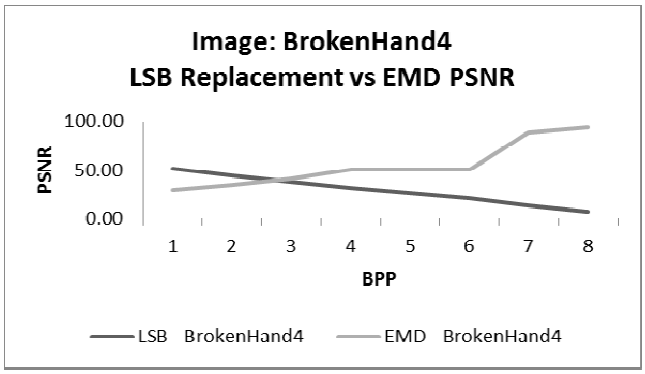


Fig 10 – BrokenHand4 - PSNR

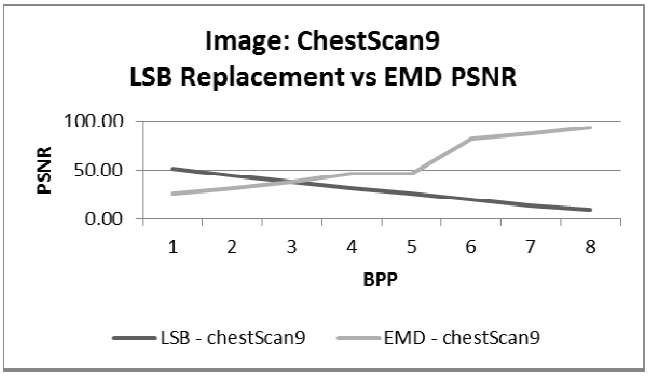


Fig 14 – ChestScan9 - PSNR

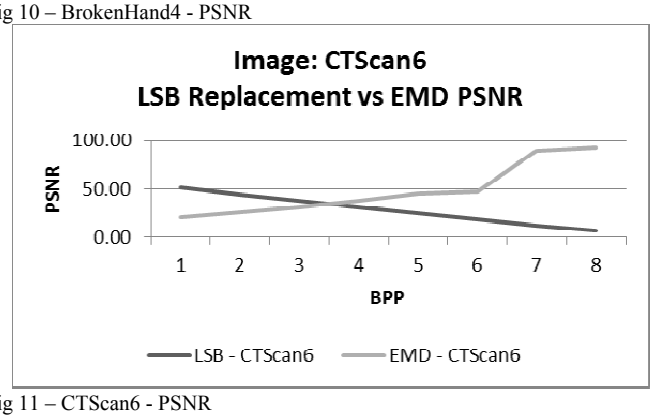


Fig 11 – CTScan6 - PSNR