IJCSI International Journal of Computer Science Issues, Volume 14, Issue 1, January 2017
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org https://doi.org/10.20943/01201701.8795

Improving Access to Radiology Health Care Services in Rural Areas of Developing Nations through a Secure Web Based Teleradiology Steganographic Method

Gabriel Kamau[1] Wilson Cheruiyot[2] and Waweru Mwangi [3]

[1] School of Computer Science and Information Technology, Dedan Kimathi University of Technology, PO box 657-10100, Nyeri, Kenya

[2&3] School of Computer Science and Information Technology, Jomo Kenyatta University of Agriculture and Technology, PO box 62000-00200, Nairobi, Kenya

Abstract

Access to specialized health care services in rural areas of developing nations and in particular sub Saharan Africa countries like Kenya is severely limited due to shortage of experts available in the medical field particularly in special domains of practice like radiology which involves professional examination of medical images e.g. X-rays and Scans (CAT, MRI etc.) for clinical interpretation and diagnosis. These experts albeit in their minimal number are only found within metropolitan areas where well-equipped referral hospitals are located.

Consequently, patients from rural areas who survive on meager incomes are forced to make high sacrifices in visiting distant referral hospitals in order to access radiology and other specialized medical services.

While it is possible to make a patient's medical images available to a practicing radiologist online e.g. through open network systems inter connectivity and email attachments, these methods don't guarantee the security, confidentiality and tamper free reliability required for a medical information system infrastructure. The possibility of securely and covertly transmitting such medical images to a remote radiologist for clinical interpretation and diagnosis through an enhanced Least Significant Bit (LSB) digital image steganographic technique was the focus of this study.

The proposed method was tested in an experimental research that involved a comparison in the carrier file's statistical properties from this technique and the traditional LSB steganographic technique of information hiding.

The study revealed improvements in imperceptibility levels in the carrier files used in this technique besides ensuring that the original MI fidelity is preserved one hundred percent by embedding it in a primary random image signal carrier file. The technique recorded a Peak Signal to Noise Ratio(PSNR) of well above 50 decibels for each image used which is well above the 30 decibels recommended for a fairly imperceptible carrier file.

Keywords: *Teleradiology,Medical Image.Staganography*

1. INTRODUCTION

The past one decade has no doubt witnessed a substantial increase in use of technology and internet connectivity across a whole range of sub Saharan African countries. This has subsequently birthed some amazing technological advances in various fields including the medical field. However in most of these countries, the most relied upon medical tool is still the old-fashioned face to face interaction with expert clinicians who have the knowledge to evaluate, monitor and care for patients.

Teleradiology is a subset of telemedicine that allows medical images to be transmitted and accessed remotely over electronic networks for clinical interpretation and diagnosis [1]. This medical technology has the potential to revolutionize access to specialized health care services in remote clinics and hospitals if properly developed and all the security and confidentiality concerns associated with it adequately addressed through continuous and progressive research [2].

In Kenya for example, a sub Saharan African country of well over forty million people, patients in rural areas seek medical care in local county clinics and dispensaries and almost in majority of the cases they are referred to the national hospitals due lack of required equipment and personnel to assist them locally.

According to [3], one of the cardinal goals of a teleradiology system is to provide timely availability of radiological images and radiologic image interpretation in emergent and non-emergent clinical care areas to facilitate radiological interpretation in on-call situations. Also teleradiology systems are used in facilitating consultative and interpretative radiology services in areas of need making services of radiologists available in medical facilities without onsite radiologist's support. This means

that highly confidential image data must be shared across computer networks among medical professionals, and researchers [1]. However, this can also expose such images to possible tampering or theft resulting to serious and costly ramifications when diagnosing ailments.

In order to ensure security in teleradiology systems, legislative rules that define the security and privacy requirements of medical information already exist. However, according to [4], these measures are not capable of providing the required security for Radiology Information Systems. Information hiding in digital files therefore present interesting possibilities and techniques that can be exploited in improving security in web based teleradiology [5],[6]. These techniques however while already well established in a wide range of other applications are only just beginning to be explored for healthcare and medical information systems [7]. Information hiding has therefore attracted considerable attention in medical image applications because of its desirable attributes [8].

2. DIGITAL IMGAE STEGANOGRAPHY

The term steganography comes from the Greek word *Steganos*, which means covered or secret and *graphy* which means writing or drawing. Literally therefore, Steganography means, covered writing. It is the art and science of writing hidden messages inside innocent looking containers such as digital images, in such a way that no one apart from the sender and intended recipient realizes the existence of a hidden message [9]. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid arousing suspicion on the existence of hidden data in a cover medium [10]. A basic technical steganographic system consists of a cover medium into which the secret message is embedded using a specific algorithm. The resultant file is called the stego media [11].

All steganographic methods and algorithms must comply with a few key requirements. The most important requirement is that a steganographic embedding method has to be imperceptible. This means that in order to effectively conceal the existence of hidden information, it is important that the embedding process does not produce perceptible distortions in the cover file. Bender related this concept to the magician's trick of misdirection, which allows "something to be hidden while it remains in plain sight" [12]. Imperceptibility also defends steganography against computer-based steganalysis by preserving certain statistical characteristics of the cover-medium. It is concerned with the stego-medium's consistency with the statistical characteristics of the original cover-file [13].

2.1 Steganography in Medical Applications

[14] States that there are at least three main goals of stego methods in medical image applications. These are:

1. The authenticity objective that helps to determine the source of a document
2. The integrity objective that helps in ascertaining that the image has not been tampered with while on transit
3. The data hiding objective which allows the inserting of the secret data so that the image is useful as a carrier file.

In order therefore to effectively achieve all the three goals of stego methods in medical image applications, there is need to strike a proper balance between capacity, robustness and imperceptibility in the carrier file.

2.2 The Traditional Least Significant Bit (LSB) Steganography Method

The traditional LSB method is one of the most commonly used steganographic methods in image steganography [10]. This method substitutes the cover image's least significant bits with the secret file bits sequentially until the entire secret file is hidden. It is based on the idea that since the LSB of any file has a place value of 1, modifying it would result in a maximum difference of only 1. Because the human eye is unable to distinguish minimal changes in color, such modifications would normally be imperceptible.

The embedding process consists of choosing a subset {j1, … , j(m)} of cover file elements and performing the substitution operation as follows:

$$LSB(Cj) = Mi \quad (Mi \text{ can be either 1 or 0}). \qquad (1)$$

Where:
j is the cover image bits
i is the secret message bits.

The embedding procedure follows the pseudo code below:

Input: Cover C

for i=1 to length (m) do

Compute index j^i where to store the i^{th} message bit of m

Sji LSB (Cji) = mi

End for

Output Stego-Object S

In the extraction process, the LSB of the selected cover file elements are extracted and used to reconstruct the secret message as shown in the pseudo code below.

Input: Stego-Object S

for i=1 to length (m) do

Compute the j^{th} cover image index where the i^{th} message bit of m is stored $m_i = LSB(C_j)$

end for

Output Message m

0	1	1
0	0	1
1	1	0
0	0	1
1	0	0
1	1	0
0	1	1
1	0	0
0	1	1
0	1	0
0	0	1
1	0	0
1	0	1
1	1	1
0	0	0
0	0	1
1	0	0
1	0	1
0	0	1
1	0	0
1	1	0
0	0	1
1	1	0
0	0	1

Fig 1. Original Bits

As [12] explains "To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the images raster data." When dealing with digital images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. The least significant bit (, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the RGB color components can be used, since they are each represented by a byte. One can therefore store 3 bits in each pixel. An 800 × 600 pixel image, can therefore store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

For example a grid for 3 pixels of a 24-bit image could be represented as shown in figure 1.

When the number 200, whose binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as shown in figure 2.

0	1	1
0	0	1
1	1	0
0	0	1
1	0	0
1	1	0
0	1	1
1	0	0
0	1	1
0	1	0
0	0	1
1	0	0
1	0	1
1	1	1
0	0	0
1	1	0
1	0	0
1	0	1
0	0	1
1	0	0
1	1	0
0	0	1
0	0	1
0	0	1

Fig 2. Modified Bits

Though the number has been embedded into the first 8 bytes of the grid, only the three highlighted bits have been changed. Mostly, only half of the bits in an image will need to be changed to hide secret data using the maximum cover size. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye - thus the message is successfully hidden.

3. PROPOSED SOLUTION

This research paper proposes an improved LSB embedding approach that uses a Random Image Signal (RIS). The RIS serves as the primary carrier file to ensure that the intactness of the MI and its 100 percent fidelity is preserved. This is because medical images meant for radiology purposes are sensitive and even the slightest alteration can result to wrong diagnosis. The MI is embedded in the spatial domain of the RIS using an enhanced LSB method The resultant stego file is then dissimulated in the primary carrier file which in this case is another MI using the enhanced LSB embedding technique. The final stego image is then transmitted to a remote radiologist who them extracts the RIS and then the patient's MI for diagnosis purposes. The general model framework adopted for the generation of the stego files based on the Birgit Pfitzmann generic model shown in figure 3.

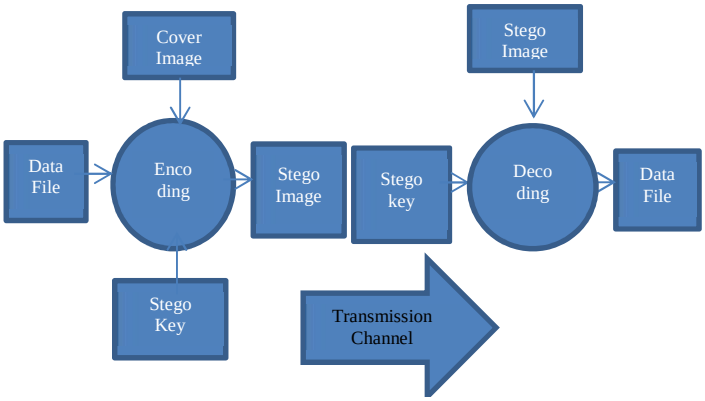

Fig 3. Model Framework.

The message digest (digital signature) of a user supplied password was used as a seed to help in pseudo-randomly picking the target image pixels and color channels for dissimulation of the MI in the carrier files using the Marsenne Twister pseudo random number generator. To further enhance imperceptibility, each pixel was decomposed into red, green and blue value octets. Each LSB of each color octet was replaced by one bit of the current MI octet. The MI octet therefore requires three pixels to be completely dissimulated. The first two pixels were used to embed the first 6 bits of the EPHI information octet. The two remaining bits were dissimulated in the third pixel's red and blue components. According to [14], human vision is more sensitive to green color changes and therefore for this pixel the green value was left unchanged.

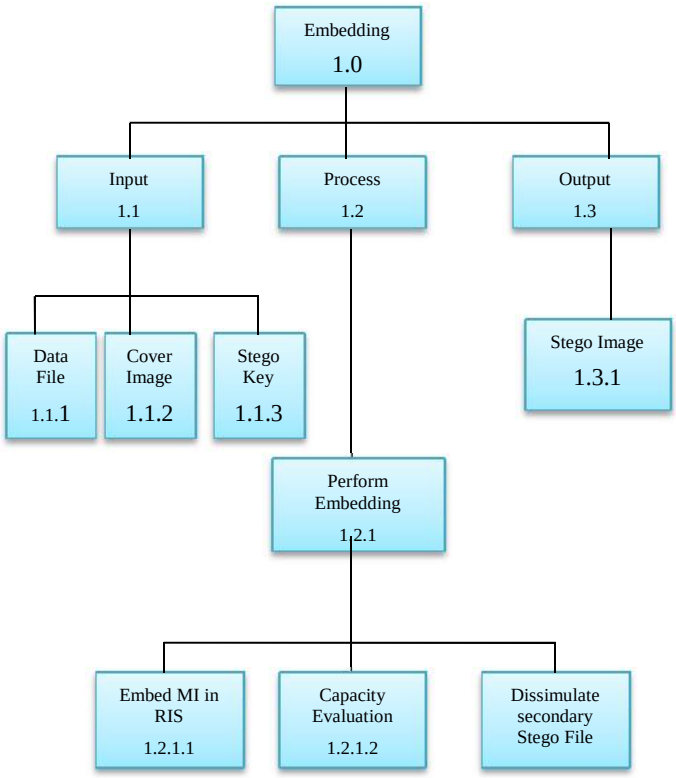

Fig 4. Hierachical I/O Diagram

Embedding Procedure

Input : Cover Image, Secret file (Payload)

Output : Stego image (image containing hidden file)

1. Use the Mersenne Twister to:

Select a random pixel

Select a random pixel color channel

Select a random color channel bit

2. Let bitToWrite [x][y][channel][bit] denote the selected bit in a specific color channel for writing

3. Let mi denote the message bit embedded in a color channel bit, bitToWrite[x][y][channel][bit]

4. For all image color channels:

5. If LSB (bitToWrite[x][y][channel][bit]) = mi then

6. Continue

7. If LSB(bitToWrite[x][y][channel][bit]) not equal to mi i then

8. bitToWrite[x][y][channel][bit] = mi

9. while secret file length; Repeat step 1 to 8 to embed the entire

Message

10. Output stego image(S)

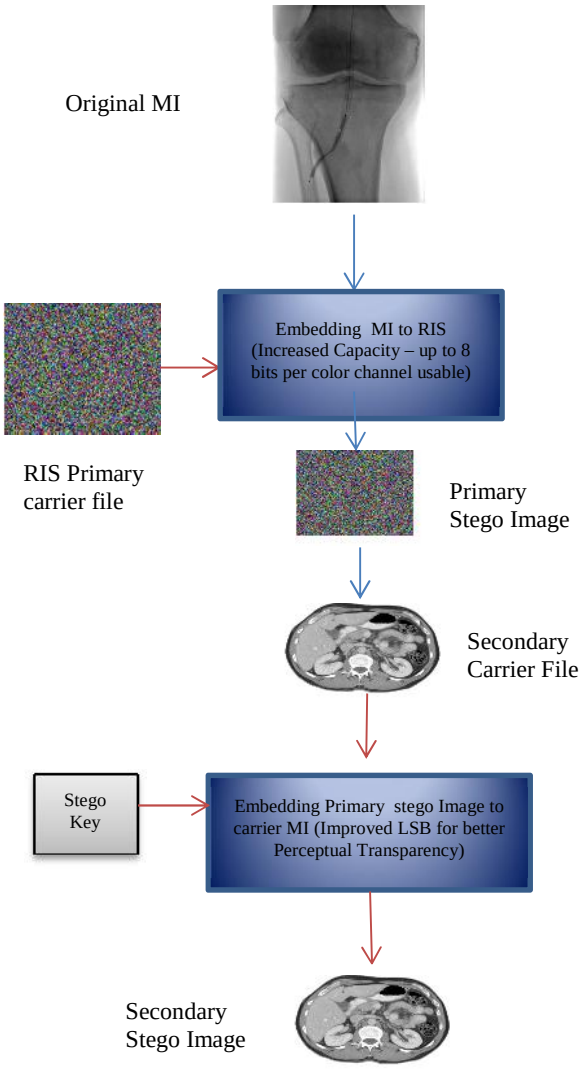

Fig 5. Embedding Procedure

Extraction Procedure

Input : Stego Image, Password message digest

Output : Secret file

Use Use the Mersenne Twister to

Select a random pixel

Select a random pixel color channel

Select a random color channel bit

2. Let bitToRead([x][y][channel][bit])denote the selected bit in a specific color channel for reading

3. Let mi denote the message bit read in a color channel bit , bitToRead([x][y][channel][bit])

4. For all image color channels;

5. If LSB(bitToRead([x][y][channel][bit]) not equal to mi then

6. Continue

7. If LSB (bitToRead([x][y][channel][bit]) = mi then

8. bitToRead ([x][y][channel][bit])= mi

9. Pack bit in bitSet

10. While secret file length; Repeat step 1 to 9 to read the entire file

11. Output secret file (M).

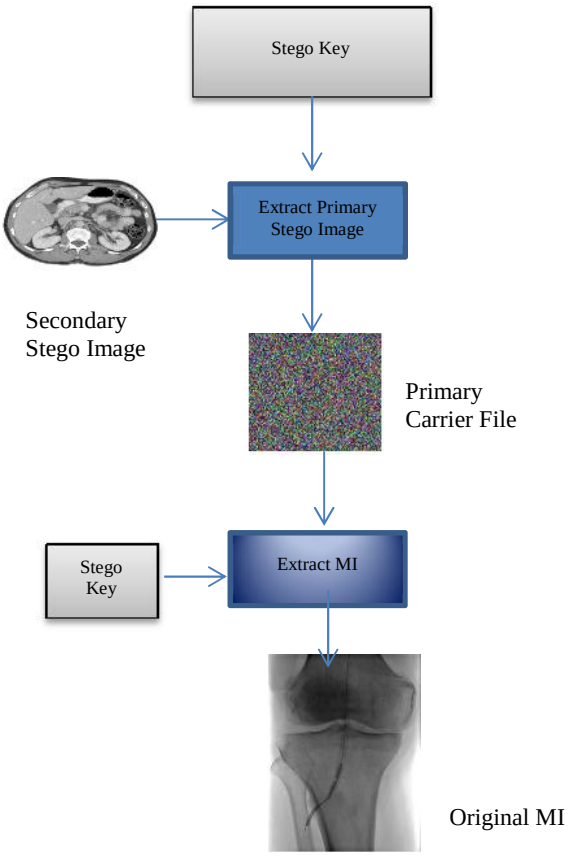

Fig 6. Extraction Procedure

4. METHODOLOGY

The aim of this study was to measure the effect of using the improved LSB encoding algorithm on imperceptibility and the payload capacity of the carrier file. Accordingly, an experimental design represented the best choice for this aim and objective.

According to [15], experimental designs should clearly outline the nature of the problem under investigation, the type of the experimental design, the implementation of the experiment, the analysis of the data, and the interpretation of the results.

Being the most accurate and obvious standard for testing a hypothesis [16], the experimental design methodology was used to achieve the main research objective. The effect of employing a randomized approach and using RIS during the embedding process represents the variable that was to be studied. Thus an experiment was carried out to test the relationship between the specific embedding process (i.e Proposed method) and the outcome in the required metric measures.

5. EVALUATION AND DISCUSSION OF RESULTS

In order to measure the effectiveness of the proposed method, the study adopted an experimental the statistical characteristics of the carrier files from the proposed method were compared with those produced by the traditional LSB method. This comparative experiment was designed to establish the robustness, the capacity and the imperceptibility of the proposed method against steganalysis and in comparison to methods that utilize the traditional LSB method.

Objective tests i.e. automated statistical analysis that examines the statistical properties of an image file were carried out on the stego images as discussed below. Statistical attacks are crucial in steganography as they are able to reveal the tiniest modifications in the statistical properties of an image [17].The following image quality metrics were employed in these tests

5.1 Peak Signal to Noise Ratio (PSNR)

PSNR measures the degree of similarity between two images (similarity of pixels). In the literature, PSNR has shown the best advantage almost over all other objective image quality metrics under different image distortion environments and strict testing conditions [18].It is defined as shown in equations (1).

$$PSNR = 10.\log_{10}\frac{I^2}{MSE}db \quad (1)$$

Where:

$$MSE = \left(\frac{1}{MN}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - \overline{X_{ij}}\right)^2 \quad (2)$$

X_{ij} is the i^{th} row and the j^{th} column pixel in the original (cover) image,

X_{ij} is the i^{th} row and the j^{th} column pixel in the reconstructed (stego) image,

M and N are the height and the width of the image

I is the dynamic range of pixel values, or the maximum value that a pixel can take, for 8-bit images: I=255.

MSE is the mean square error.

5.2 Signal to Noise Ratio (SNR)

This is an objective quality evaluation metric whose measures are estimates of the quality of the stego image compared with the original image. The larger the value of SNR the higher the imperceptibility level of the embedding algorithm [19].

$$SNR = 10 * Log_{10}\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(A_{ij}\right)^2}{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(A_{ij} - B_{ij}\right)^2} \quad (3)$$

Where:

A_{ij} represents one pixel in the original image (before embedding the data)

B_{ij} represents one pixel in the stego image (after embedding the hidden data).

5.3 Reed-Solomon (RS) Analysis

RS measures the smoothness of the changes among pixels (the lower the value, the smoother the changes among them, or the lesser the noise of the image). RS is one of the most reliable quantitative steganalysis methods [13]. RS analysis is derived from what the authors refer to as R, i.e. Regular blocks, and S, i.e. Singular blocks. The term regular comes from the fact that what is happening is what it is expected, while singular comes from not being expected. What should be expected is, for images that have not being subject to steganography, the number of pixel blocks of R type subject to a positive increase would be approximately equal to those experiencing a negative increase. And the same for S blocks. In images with hidden information, the authors observe that the difference between R blocks with positive and negative modifications is increased, while the difference between S blocks with positive and negative modifications is decreased. It is defined as shown in equation (3)

$$R_M \cong R_{-M} \text{ and } S_M \cong S_{-M} \quad (4)$$

5.4 Test Data

Images shown in table 2 were used in conducting the experiment. Any digital image can also be used in this experiment. A common primary carrier image was used as shown in table 3. The use of a common primary carrier file was to enable the researcher compare the distortion levels of this carrier file under the two different algorithm and thereby be able to the research conclusions.

Table 1: Test data Images

FILE NAME	DIMENSIONS	FILE SIZE
Brain.gif	286 x 233	48KB
x-ray lumbar .jpg	537 X 867	106KB
fluoroscopy.jpg	472 X 633	112KB
vessels-knee.jpg	244 X 417	46 KB

Table 2: Secondary carrier Image

FILE NAME	DIMENSIONS	FILE SIZE
Pulmonary.jpg	820 x 720 Pixels	113KB

6. TEST RESULTS

Table 3: PSNR and SNR Results for the Traditional LSB method

IMAGE FILE	SIZE (kb)	DIMENSION	RS Analysis(Db)	PSNR (dB)	SNR (dB)
Brain.gif	48	286 X 233	28	59	52
X-ray lumber.jpg	106	537 X 867	51	56	49
Fluoroscopy.jpg	112	472 X 633	50	56	49
Vessel-Knee.jpg	46	244 X 417	23	59	53

Table 4: PSNR and SNR Results for the Proposed Solution

IMAGE FILE	SIZE (kb)	DIMENSION	RS (dB)	PSNR (dB)	SNR (dB)
Brain.gif	48	286 x 233	25	61	54
X-ray lumbar.jpg	106	537 X 867	52	57	50
fluoroscopy .jpg	112	472 X 633	49	57	50
vessels-knee.jpg	46	244 X 417	24	61	55

6. 1 PSNR Comparative Analysis

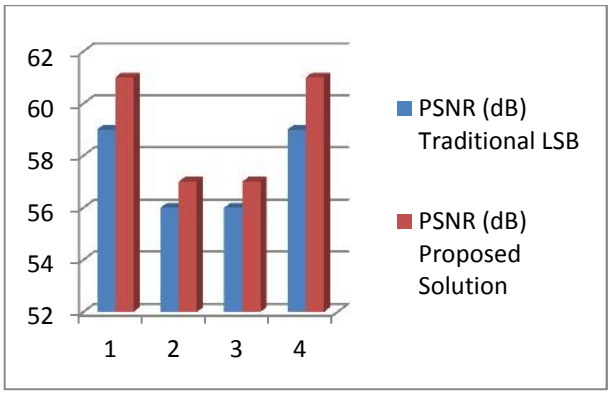

Fig 7. Comparative Analysis - Peak Signal to Noise Ratio

Every image tested registered a higher PSNR when the proposedd LSB was used compared to when the Traditional LSB was used. These results therefore clearly shows that the proposed LSB embedding method improves on imperceptibility of the hidden data since a higher Peak Signal to Noise Ratio (PSNR) always indicates improved imperceptibility[19].

6. 2 SNR Comparative Analysis

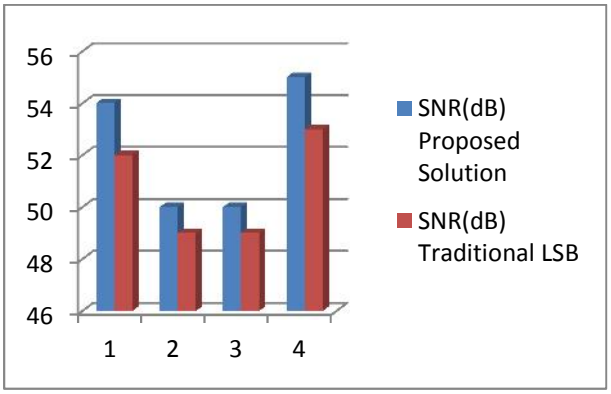

Fig 8. Comparative Analysis Signal to Noise Ratio

Again for all the four test data images used, each registered a higher SNR when the proposed LSB method was used compared to when the Traditional LSB method was used. For any embedding algorithm or method, the larger the value of SNR the higher the imperceptibility level [19]. These results therefore establish the superiority of the proposed method compared to the traditional LSB Method.

6. 2 RS Comparative Analysis

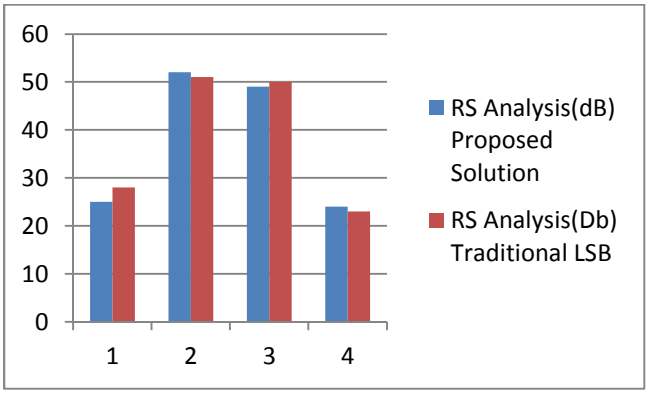

Fig 9. Comparative Analysis Read Solomon Analysis

According to [13] RS measures the smoothness of the changes among pixels (the lower the value, the smoother the changes among them, or the lesser the noise of the image). Stego images generated by the proposed method all recorded lower values of RS compared to those generated by the traditional LSB method. Therefore these images have lesser noise and the information hidden in them more imperceptible.

6.3 Histogram Analysis

Histogram analysis of the carrier images was carried out in order to detect and compare changes in frequency of appearance between the original images and the stego images as produced by the two techniques. Stego images from the proposed technique showed the least change compared to the histogram of the original images.

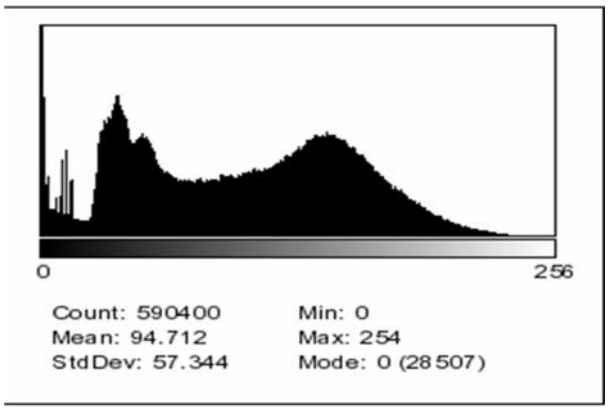

Fig 10. Original Carrier (Secondary) Image

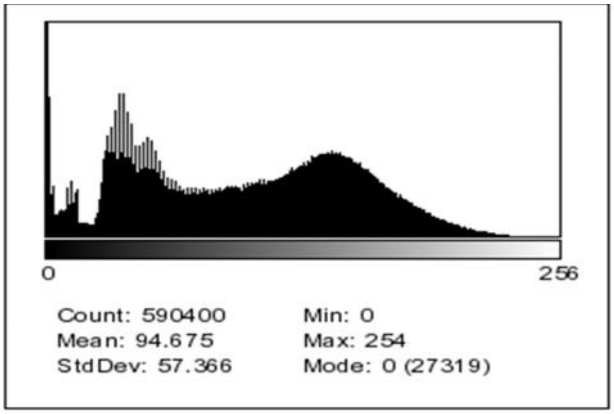

Fig 11. MI (Brain.GIF) embedded using Traditional LSB method

MI (Brain.GIF) embedded using proposed technique

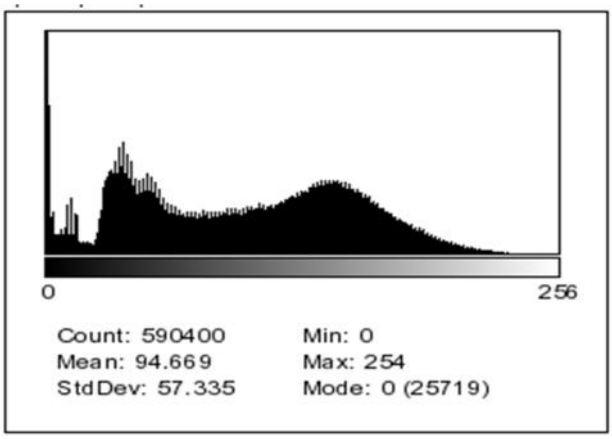

Fig 12. MI (Brain.GIF) embedded using Proposed Technique

7. CONCLUSION

This research set out to investigate on an enhanced steganographic method that can be used in improving the security in web based teleradiology systems in the quest of improving health care access to rural population in developing nations. The impact of using the image's randomly targeted bits in the LSB steganography method embedding process on imperceptibility and undetectability of hidden data was tested and demonstrated. The test results for various image metrics showed that using this technique for image bits swapping during the embedding process significantly improves on the imperceptibility and the undetectability of the hidden data thereby ensuring better security of the MI transmitted through a web based teleradiology infrastructure. Based also on experiment results discussed earlier, this steganographic embedding process results in comparatively lesser distortion and noise in the original cover image signal as opposed to the traditional method. The analysis of the statistical differences as discussed using the various image metrics reveals that using the proposed enhanced method leads to lesser statistical differences between the original image and the carrier image. This means improvement to both visual and statistical imperceptibility of the hidden data. By using RIS instead of an ordinary image as the primary carrier file, the proposed method ensures that the MI is received intact by the remote radiologist ensuring that correct diagnosis is guaranteed as the original image is not interfered with by embedding data or a watermark directly into it. Also, the possibility of using all the eight bits in each pixel of the RIS significantly increases its payload capacity as a secondary carrier file.

7. REFERENCES

[1] Nyeem, Hussain, Wageeh, Boles, & Boyd, Colin. 2013. A review of medical image watermarking requirements for teleradiology. Journal of Digital Imaging, 26(2), pp. 326-343.

[2] Prior. F, M. L. Ingeholm, B. A. Levine, and L. Tarbox. 2012. Potential impact of HITECH security regulations on medical imaging. Annual International Conference of the IEEE Engineering in Medicine and Biology Society. Piscataway, NJ, USA, 2009, pp. 2157-60

[3] Madennis Michael.2009. Security in Teleradiology Systems. University of Arizona.

[4] Kobayashi. L and S. S. Furuie.2009. Proposal for DICOM multiframe medical image integrity and authenticity," Journal of Digital Imaging, vol. 22, pp. 71-83.

[5] Q. Li and N. Memon.2010. Security Models of Digital Watermarking, in Multimedia Content Analysis and Mining. vol. 4577, N. Sebe, Y. Liu, Y. Zhuang, and T. Huang, Eds., ed: Springer

[6] R. Chandramouli, N. Memon.2011. Analysis of LSB Based Image Steganography Techniques. IEEE pp. Springer Verlag, 347-350..

[7] D. Que, X. Wen, and B. Chen.2011. PACS model based on digital watermarking and its core algorithms. in MIPPR 2009 - Medical Imaging, Parallel Processing of Images, and Optimization Techniques: 6th International Symposium on Multispectral Image Processing and Pattern Recognition, Huazhong University of Science and Technology; National Natural Science Foundation of China; China Three Gorges University.

[8] Das. S and Kundu.2010.Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding," in Pattern Recognition (ICPR), 20thInternational Conference on, 2010, pp. 1457-1460.

[9] Gabriel Macharia Kamau, Stephen Kimani, and Waweru Mwangi, "An enhanced Least Significant Bit Steganographic Method for Information Hiding ", Journal of Information Engineering and Applications, Vol. 2, No.9, 2012, pp. 1-12..

[10] Neil, F. J. and Jajodia, S. 1998. Exploring Steganography: Seeing the Unseen', IEEE Computer, 31(2), pp 26-34.

[11] Sellars D.2006) .An Introduction to Steganography," http ://www. totse.com /en/privacy/ encryption/ 163947. Html Bender, W. 1996. Techniques for Data Hiding', IBM Systems Journal, 35(3&4), pp 313-336.

[12] Fridrich, J., Goljan, M. and Du, R. 2001. Reliable Detection of LSB Steganography in Color and Grayscale Images. IEEE Multimedia. 8, 22-28.

[13] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux.2006. A Review of Image Watermarking Applications in Healthcare," in Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE, 2006, pp. 4691-4694.

[14] C. Cachin. 2008. An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318.

[15] Hinkelmann, K. & Kempthorne, O. 2008 Design and Analysis of Experiments: Introduction to Experimental Design, John Wiley & Sons, Inc., Hoboken,New Jersey.

[16] Shuttleworth, M. 2008. Experiment Resources. Accessed: June 3rd , 2016. URL:http://www.experiment-resources.com.

[17] Artz, D. 2011. Digital steganography: hiding data within data", *Internet Computing, IEEE*, vol. 5, Issue: 3, pp. 75-80

[18] Wang, Z., Bovik, A. C. and Lu, L. 2002a. Why is image quality assessment so difficult? IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '02), 4, 3313-3316.

[19] Mei Jiansheng, Li Sukang and Tan Xiaomei.2009. A Digital Watermarking Algorithm Based on DCT and DWT", in Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, pp. 104-107.