Towards A More Secure Web Based Tele Radiology System: A Steganographic Approach

Gabriel Kamau *gabriel.kamau@dkut.ac.ke*
School of Computer Science and Information Technology
Dedan Kimathi University of Technology
Nyeri, 10100,Kenya

Wilson Cheruiyot *wilchery68@gmail.com*
School of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
Nairobi,00200,Kenya

Waweru Mwangi *waweru_mwangi@icsit.jkuat.ac.ke*
School of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
Nairobi,00200,Kenya

Abstract

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 in a medical information system infrastructure. The possibility of securely and covertly transmitting such medical images remotely for clinical interpretation and diagnosis through a secure steganographic technique was the focus of this study.

We propose a method that uses an Enhanced Least Significant Bit (ELSB) steganographic insertion method to embed a patient's Medical Image (MI) in the spatial domain of a cover digital image and his/her health records in the frequency domain of the same cover image as a watermark to ensure tamper detection and nonrepudiation. The ELSB method uses the Marsenne Twister (MT) Pseudo Random Number Generator (PRNG) to randomly embed and conceal the patient's data in the cover image. This technique significantly increases the imperceptibility of the hidden information to steganalysis thereby enhancing the security of the embedded patient's data.

In measuring the effectiveness of the proposed method, the study adopted the Design Science Research (DSR) methodology, a paradigm for problem solving in computing and Information Systems (IS) that involves design and implementation of artefacts and methods considered novel and the analytical testing of the performance of such artefacts in pursuit of understanding and enhancing an existing method, artefact or practice.

The fidelity measures of the stego images from the proposed method were compared with those from the traditional Least Significant Bit (LSB) method in order to establish the imperceptibility of the embedded information. The results demonstrated improvements of between 1 to 2.6 decibels (dB) in the Peak Signal to Noise Ratio (PSNR), and up to 0.4 MSE ratios for the proposed method.

Keywords: Imperceptibility, Steganalysis, Steganographic,Radiologist, Decibels.

1. INTRODUCTION

The past one decade has witnessed an increase in automation of medical records by health care providers with the intent of making the sharing of such information among the various stakeholders more efficient and reliable. This has birthed new possibilities and practices in the medical field among them telemedicine and tele radiology.

Tele radiology 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 no doubt has the potential to revolutionize access to specialized health care services in developing nations of the world where there is severe shortage of experts particularly in special domains of medical practice like radiology.

According to [2], one of the cardinal goals of tele radiology systems 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 tele radiology 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 and Electronic Patient Health Information (EPHI) and data must be shared across computer networks among medical professionals, and researchers [1]. However, this also exposes such data to possible tampering or loss which can result to serious and costly ramifications. In order to ensure security in tele radiology systems, legislative rules that define the security and privacy requirements of medical information already exist. However, according to [3], these measures are not capable of providing the required security for radiology information systems.

Information hiding in digital files present interesting possibilities and techniques that can be exploited in improving security in web based tele radiology [4].

2. STEGANOGRAPHY IN MEDICAL APPLICATIONS

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 is aware of the exchange of data [5].

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 [5]. A basic technical steganographic system consists of a cover medium into which the secret message is embedded using a specific method, technique or algorithm. The resultant file is called the stego media [6].

Besides ensuring that the source of images used is standardized [7], a steganographic technique must also comply with basic standards for steganography. 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" [8]. High levels of imperceptibility means that minimal distortions are introduced in the original cover image during the embedding process ensuring that its fidelity is maintained. Steganalysis then becomes fairly difficult when this is observed [9].

According to [10], 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 for imperceptible insertion of the secret data so that the image is useful as a carrier file.

The proposed method meets the first and the second objective by embedding a watermark signature generated by the patient's Electronic Health Information (EHI) in the transform domain of the cover file. The signature is then used upon extraction to provide authenticity of the MI received. The extracted signature is also used to test for any tampering with the cover file which would obviously compromise the MI. The used MT PRNG in enhancing and improving the embedding procedure meets the third goal of stego methods in medical image applications.

2.1 The Traditional Least Significant Bit (LSB) Steganographic Method

The traditional LSB method is one of the most commonly used steganographic methods in image steganography [11]. 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 [12].

The embedding process involves a procedure of choosing a subset {j1, …, j(m)} of cover image bits and performing a substitution operation as follows:

LSB(Cj) = Mi (Mi can be either 1 or 0). (1)

Where:
Cj is the cover image bit
Mi is the secret message bit

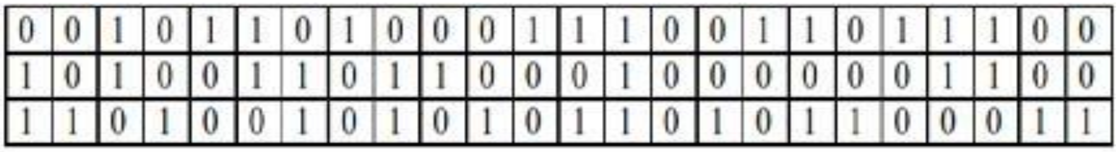
The summary of the entire embedding procedure is outlined below.

```
Input: Cover Image (C)
for i =1 to the length of the secret file (M) do
Compute index ji where to store the ith message bit of M
Sji → LSB (Cji) = Mi
End for
Output Stego-Object (S)
```

In the extraction process, the LSBs of the selected cover file are extracted and used to reconstruct the secret message as outlined below.

```
Input: Stego-Object (S)
for i=1 to the length of the secret file (M) do
Compute the jth cover image index where the ith message bit of M is stored
Mi = LSB (Cj)
end for
Output Message (M)
```

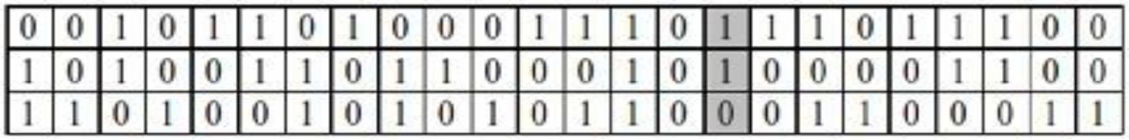
As [8] explains, to a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the images raster data. When dealing with digital images for use with steganography, 8-bit and 24-bit per pixel image files are typical. The least significant bit (in other words, 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 Red, Green and Blue colour 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 [13]. For example a grid for 3 pixels of a 24-bit image could be represented as shown in figure l.



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

FIGURE 1: Pixel Bits Before Embedding.

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 will be as shown in FIGURE 2 with highlighted section showing the bits affected



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

FIGURE 2: Pixel Bits After Embedding.

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. With a well-chosen image, one can even hide the message in the least as well as the second least significant bit and still not see the difference [14].

The sequential insertion pattern employed by the LSB method during the embedding process means that the imperceptibility level to the concealed data is relatively low. This is because the cover image will tend to be degraded along the section of the image where the data is embedded. Through steganalysis software tools, an attacker can easily destroy the hidden data by removing or zeroing the entire LSB plane with very little change in the perceptual quality of the modified stego-image.

The conventional LSB algorithm is also very sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, addition of noise, or lossy compression to the stego-image will normally destroy the message. It also has low support for a variety of image file formats.

3. METHODOLOGY

The main aim of this research was to investigate on the requirements for a secure LSB based steganographic method that enhances on the imperceptibility levels of the traditional LSB method and which is adaptable to the needs of a web based tele radiology infrastructure. Design Science Research (DSR), a “learning through building artefact construction” research method was therefore considered the most productive and accurate for this study. According to [23], DSR is “a research activity that invents or builds new, innovative artefacts for solving problems or achieving improvements on existing methods. DSR creates new means for achieving some general goal, as its major research contributions. Such new and innovative artefacts create new reality, rather than explaining existing reality or helping to make sense of it. It is a paradigm for problem solving in computing and Information Systems (IS) that involves design and implementation of artefacts considered novel and the analytical testing of the performance of such artefacts in pursuit of understanding and enhancing an already existing artefact or practice[24]. According [25], DSR has become an accepted methodology for research in IS and its importance in creating and evaluating Information

Technology artefacts intended to solve identified organizational problems is well established [26] . It provides a roadmap for researchers who want to use design as a research mechanism for IS and computing research.

Being a problem solving paradigm in IS and computing where analytical techniques assist in carrying out research, DRS follows a “learning through building artefacts approach”. It involves design of Information Technology (IT) artefacts and IS systems with the aim of increasing their usefulness and the analysis of the performance of such creations with the aim of enhancing the behavior of given aspects of the system under study [24].

4. PROPOSED METHOD

The proposed ELSB steganographic insertion method embeds a patient’s MI in the spatial domain of a carrier image and his/her health records in the frequency domain as a watermark to ensure tamper detection and nonrepudiation. It employs a selective and randomized approach in picking target image bits in the carrier image using the Mersenne Twister (MT) pseudo random number generator (PRNG). The selected carrier image bits are then swapped with the patient’s data bits to effectively embed the patient’s data in the carrier image.

4.1 Marsenne Twister (MT)

MT is a pseudorandom number generator developed by Makoto Matsumoto and Takuji Nishimura in 1997. It provides for fast generation of very high-quality pseudorandom numbers with a long period length which is chosen to be a marsenne prime. Other advantages of MT include high order of dimensional equidistribution, high speed of random numbers generation and reliability [16]. As of January 2016, 49 Marsenne primes are known including the largest known prime number 274,207,281 − 1 which is a Marsenne prime [15]. It has a period of 2^19937-1.

4.2 The Algorithm

The MT algorithm is a twisted generalized feedback shift register (twisted GFSR, or TGFSR) of rational normal form (TGFSR(R)), with state bit reflection and tempering [17]. It is based on the following linear recurring equation.

$$x_{k+n} = x_{k+m} \oplus (x_k^{u} \mid x_{k+1}^{l})A \quad (k=0,1,\ldots) \qquad (2)$$

Where:
n is the degree of occurrence
k is 0,1,2,……
xn is a row vector of a word size w, which is generated when k = 0
x0, x1,….. xn-1 are initial seeds
m is a middle term where $1 \leq m \leq n$
A is a *wxm* matrix, whose form is chosen to ease the matrix
multiplication
r is the number of bits masked or a separation point of one
word , $0 \leq r \leq w-1$
u is upper or leftmost bits
l is lower or rightmost bits

The concatenation of the $x_{k,}$ upper bits and x_{k+1} lower bits yields a *w* dimensional vector making it possible for the matrix *A* to be multiplied from right [22]. Multiplication is carried out through simple bit shifting operations while concatenation is computed using a bitwise AND operation.

The sequences generated by the linear recurring equation have poor high dimension equidistribution. A final technique called “tempering” that improves this is applied to produce the final pseudorandom sequence. A wxm invertible matrix T is multiplied with each generated word from the right, yielding a result of the transformation of x into z=xT [23].

The tempering matrix T is uniquely chosen to enable the binary operations to be performed as follows:
y = y (y>>u)
y = y (y<<s) & b
y = y (y<<t) & c
y = y (y>>l)
Output y

Where:
u,s,t and l are tempering bit shifts
b,c are tempering bitmasks
<< denotes a bitwise left shift
>> denotes a bitwise right shift
& denotes a bitwise AND operation

The following is the summary of the MT32 parameters which are carefully chosen in order to attain the properties mentioned above [24].

Parameters	Quantity
N	624
W	32
R	31
M	397
A	99083B0DF16
U	11
S	7
T	15
L	18
B	9D2C5680
C	EFC60000

TABLE 1: 32-BIT MT 19937 Parameters.

Where:
W is the word size (in number of bits) N is the degree of recurrence
M is the middle word, or the number of parallel sequences,
1 ≤m ≤n
R is the separation point of one word, or the number of bits of the lower bitmask, 0 ≤r ≤w - 1
A is the coefficients of the rational normal form twist matrix
B, C are the TGFSR(R) tempering bitmasks
S, T are the TGFSR(R) tempering bit shifts
U, L are the additional Mersenne Twister tempering bit shifts

Where:
W,N,M and R = 32,624,397 and 31 respectively.
a = 9908B0DF16
(S,B) = (7,9D2C568016)
(t,c) = (15,EFC6000016)
U = 11
l = 18

The feedback shift register is composed of 624, 32-bit length elements and a total of 19937 cells [18]. The complete pseudo code is outline below.

```
// Create a length 624 array to store the state of the generator
int[0..623] MT
int index = 0
// Initialize the generator from a seed function initializeGenerator(int seed) { MT[0] := seed
    for i from 1 to 623 { // loop over each other element
        MT[i]  := last  32 bits  of(1812433253  *(MT[i-1]  xor (right shift by 30 bits(MT[i-1]))) + i) // 0x6c078965
    }
}
/* Extract a tempered pseudorandom number based on the index-th value, calling
generateNumbers()  every 624 numbers */
function extractNumber() { if index == 0 { generateNumbers()
    }
    int y := MT[index]
    y := y xor (right shift by 11 bits(y))
    y :=  y xor  (left  shift  by 7 bits(y)  AND  (2636928640))  // 0x9d2c5680
    y := y xor (left shift by 15 bits(y)  AND (4022730752))  // 0xefc60000
    y := y xor (right shift by 18 bits(y))
    index := (index + 1) mod 624 return y
}
// Generate an array of 624 untempered numbers
function generateNumbers()  {
    for i from 0 to 623 {
        int y := 32nd bit of(MT[i]) + last 31 bits of (MT[(i+1) mod 624])
        MT[i] := MT[(i + 397) mod 624] xor (right shift by 1 bit(y))
        if (y mod 2) == 1 { // y is odd
            MT[i] := MT[i] xor (2567483615) // 0x9908b0df }
    }
}
```

4.3 Watermarking

The frequency domain of the carrier image was used for embedding the patient's EPHI as watermark. This ensures that the hidden data resides in the more robust areas, spread across the entire image providing better resistance against signal processing operations [21]. In particular 2D Haar Discrete Wavelength Transform was applied in order to isolate the high resolution sub bands (edges) of the image. DWT has special frequency localization and therefore any change in its transform coefficients affects the local sub- band and not the entire image. DWT techniques generally represent the mathematical tool for the hierarchical deposition of an image capturing both the frequency and the location information of the image signal [22]). The image is specifically decomposed into three spatial directions i.e. Vertical, Horizontal and Diagonal. The resultant wavelets represent more precisely the anisotropic properties of Human Visual System (HVS). The input image is divided into four none overlapping multi- resolution sub-bands i.e. LL1, representing the lowest sub-band which contains the low frequency wavelet coefficients containing the significant part of the spatial domain image, and LH1, HL1, and HH1 representing the vertical details, the horizontal details and diagonal details.

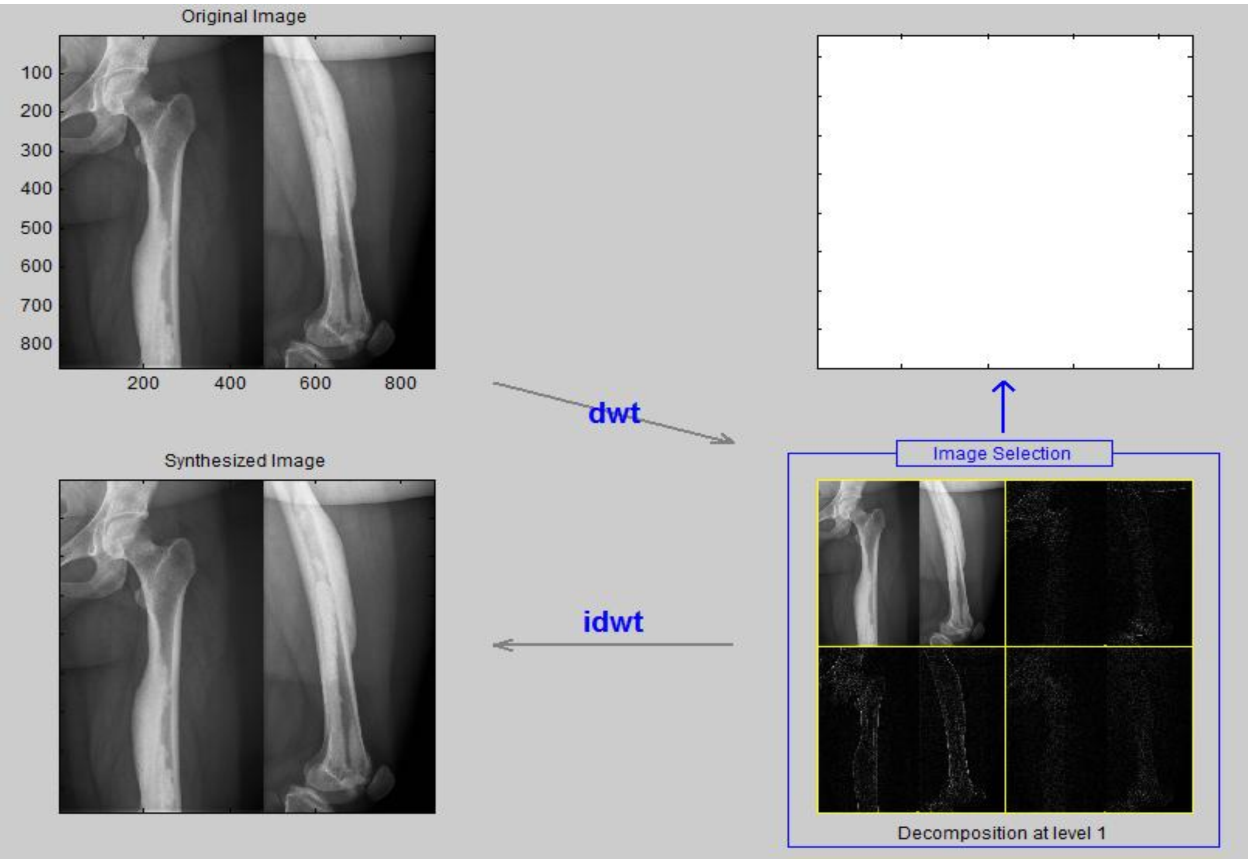


FIGURE 3: DWT Level 1 Decomposition.

The magnitude of DWT coefficients is larger in the lowest sub-bands at each level of decomposition and is smaller for other sub-bands [22]. The discrete wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis.

4.3 Embedding Procedure (Patient's EPHI)

The patient EPHI is embedded in the transform domain of the cover file as a watermark using Haar DWT. The complete embedding procedure is outline below.

Input: An m × n Cover image (C) and a signature file (EPHI)
Output: An m × n stego-image .
Algorithm: Steps-
1. Input the cover image (C)
2. Calculate the size of cover image
3. Read the watermark signature file (F)
5. Decompose C by using Haar DWT wavelet transform
7. Modify detailed coefficients of wavelet decomposition by adding F
8. Apply inverse DWT (to reverse to spatial domain)
9. Output Stego Image (S1)

The patient's MI is then embedded in the spatial domain of the same cover file using the ELSB method. The complete embedding procedure is outline below.

Input: An m x n Stego Image (S1) , MI file (Payload)
Output: Stego image (S2)
Algorithm: Steps-1.

```
1. Use the Marsenne Twister to select a random color channel bit (in cover image)
2. Let bitToWrite [x][y][channel][bit]  denote the selected bit in a specific color channel for writing
3. Let mi denote the patient's data 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 continue
6. If LSB(bitToWrite[x][y][channel][bit])  not equal to mi
then
8. bitToWrite[x][y][channel][bit] = mi
9. While secret file length; Repeat step 1 to 8 to embed the
entire patients Image(MI)
10. Output stego image(S2).
```

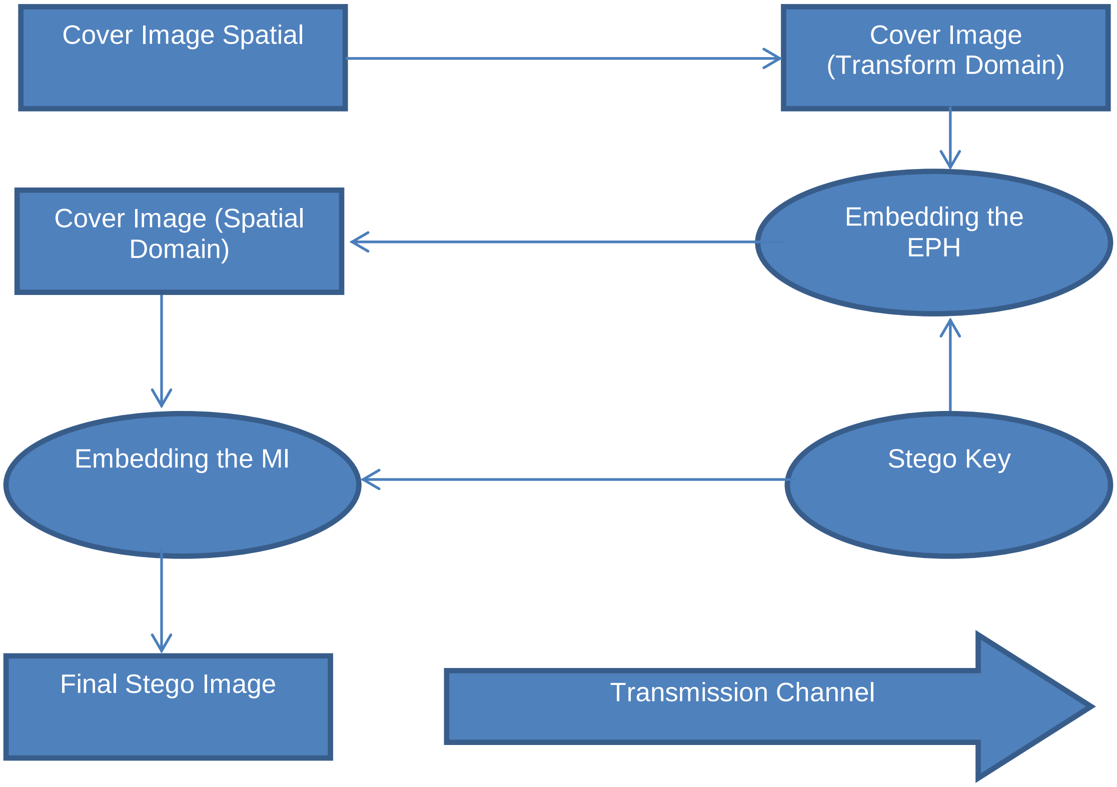


FIGURE 4: Embedding Process.

4.3 Extraction Procedure

The cover file is initially tested for tampering and also to authenticate the source. This procedure is outlined below.

Input: Stego Image (S2) (EPHI Watermarked image containing MI)
Output: EPHI,,Nonrepudiation, tamper test
Algorithm: Steps-

```
1. Read the Stego image
2. Read the Signature file (F)
3. Decompose the S2 using Haar DWT wavelet transform
4. Compare Signature file (F) read with that embedded in the stego image
5. Output validity of signature in percentage (to take care of any distortions occasioned  by noise
or otherwise
```

If no tempering is detected, the patient's data (MI and EPHI) is extracted and used in diagnosis or archiving. This procedure is outline below.

```
Input:   Stego   Image (S2) (EPHI   Watermarked   image containing MI)
Output: MI
Algorithm steps.
1. Use the Mersenne Twister to select a random color channel bit
2. Let bitToRead([x][y][channel][bit]) denote the selected bit  in a specific colour channel for
   reading
3. Let mi denote the patient's data bit read in a colour channel bit, bitToRead([x][y][channel][bit])
4. For all image colour channels;
5. If LSB(bitToRead([x][y][channel][bit]) not equal to mi then , 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 patient's data file length; Repeat step 1 to 9 to read the entire file
11. Output patient's data (MI and EPHI).
```

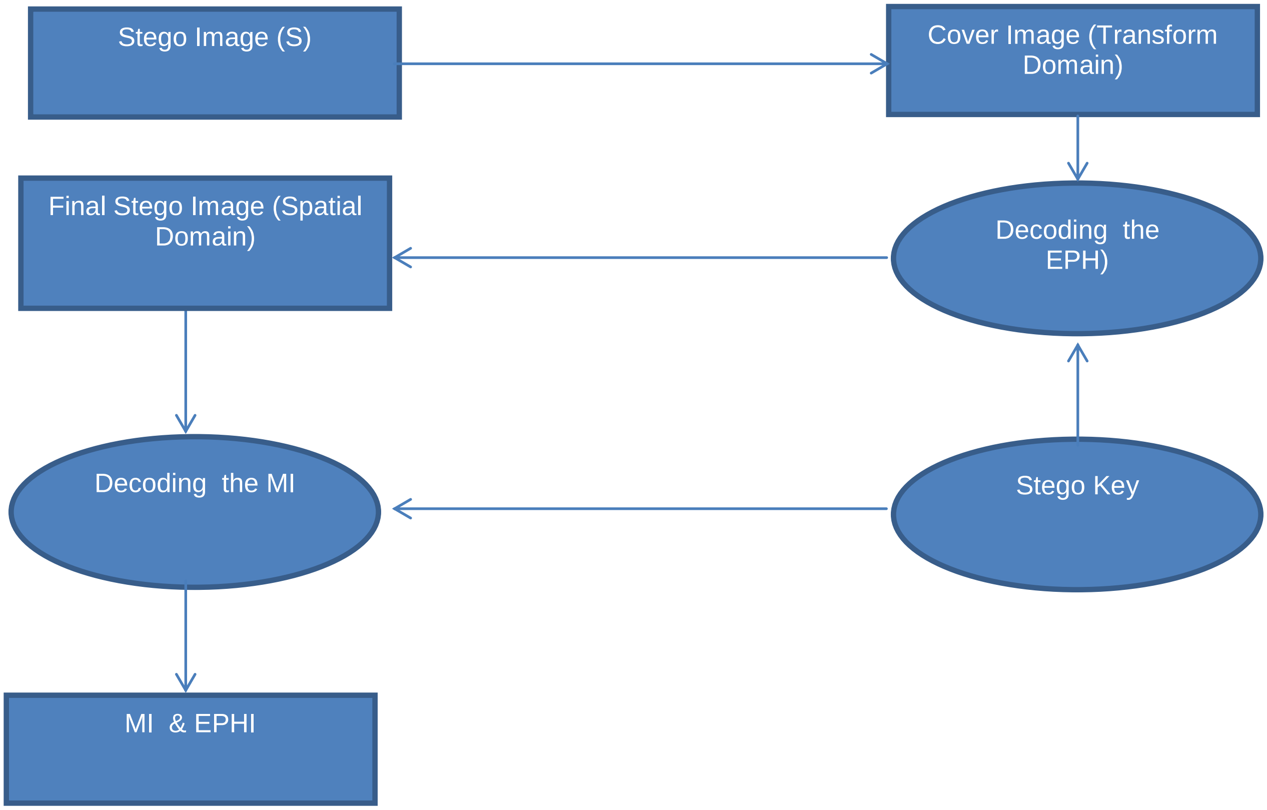


FIGURE 5: Extraction Process.

5. EVALUATION AND DISCUSSION OF RESULTS

Thirteen MI payloads were used as test data files in five different cover files. The results were analyzed using the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) full reference image quality analysis metrics. Full reference image quality metrics are error sensitivity measures and are meant to establish the errors or image signal differences between the stego and the original reference images [27].

FILE NAME	DIMENSIONS	FILE SIZE	COMMENT
Image1.	521 x 1222	52 KB	Payload1
Image2.	959 x 1222	142 KB	Payload 2
Image3.	970 x 1945	243KB	Payload 4
Image4.	1215 x 1041	393 KB	Payload 6
Image5	640 x 2237 P	440 KB	Payload 7
Image6	785 x 2001	573 KB	Payload 9
Image7	761 x 2412	617 KB	Payload 11
Image8	1079 x 194	747 KB	Payload 13

TABLE 2: Test Data Images – Payloads (MI).

This comparative experiment was for carrying out a comprehensive objective testing to establish the differences and or similarity in fidelity between the original and the stego image signals as produced by both the traditional LSB method and the proposed method

5.1 Mean Square Error (MSE)

This is the most commonly used full reference image quality metric. It is computed by averaging the squared intensity differences of the reconstructed and the reference image pixels [28].It measures the error with respect to the center of the image values i.e. the mean of the pixel values of the image by averaging the sum of the squares of the error between two images [29].

According to [28], advantages of MSE include the fact that it is simple to calculate, it has a clear physical meaning and it is mathematically convenient in the context of optimization.

If the value of MSE is lower, it implies that there is less number of errors in the reconstructed signal [30]. For an image with a size of (M x N), the value of MSE is expressed as shown in Equation 3 [31]

FILE NAME	DIMENSIONS	FILE SIZE
CoverImage1	900 x 600	277 KB
CoverImage2	2048 x 1368	323 KB
CoverImage3	2048 x 1458	414 KB
CoverImage4	1936 x 1288	504 KB
CoverImage5	3735 x 1071	591 KB

TABLE 3: Test Data Images – Cover Images.

$$MSE_{AVG} = \frac{1}{\left(MN\right)} \sum_{i=1}^{M} \sum_{J=1}^{N} \left(Xij - \overline{Xij} \right)^2 \qquad (3)$$

Where:

MSER = MSE for Red component
MSEG = MSE for Green component
MSEB = MSE for Blue component

According to [34], MSE as a metric for image quality analysis possesses some characteristics that make it a widely used performance measure in the field of signal processing. These characteristics include the fact that it has a physically clear meaning, i.e., it is a natural way of defining the energy of an error signal. It is also a simple and computationally inexpensive method.

Lastly, since MSE satisfies properties like convexity, symmetry, and differentiability, it is considered as an excellent measure in optimization applications.

According to [33], MSE as a metric for image quality analysis possesses some characteristics that make it a widely used performance measure in the field of signal processing. These characteristics include the fact that it has a physically clear meaning, i.e., it is a natural way of defining the energy of an error signal. It is also a simple and computationally inexpensive method. Lastly, since MSE satisfies properties like convexity, symmetry, and differentiability, it is considered as an excellent measure in optimization applications.

5.2 Peak Signal to Noise Ratio (PSNR)

PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation normally represented in decibels [22]. It is one of the most extensively used metric parameter for the measurement of the quality of a reconstructed image [34]. There is a distinct inverse relation between MSE and PSNR. The Lower the MSE, the higher the PSNR. The PSNR value approaches infinity as the MSE approaches zero; this shows that a higher PSNR value is desirable as it literally means that the ratio of the image signal to noise is more providing a higher image quality. At the other end of the scale, a small value of the PSNR implies high numerical differences between images [35]. The value of PSNR is computed using equation (5)

$$PSNR = 10.\log 10 \frac{I^2}{(MSE)} db \qquad (4)$$

Where:

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

MSE is the Mean Square Error representing the cumulative squared error between the original image signal and the stego-image signal.

5.3 Results and Discussion

In all the payloads embedded in the five cover images, the proposed method posted higher levels of MSE ratios indicating comparative less distortion to the original cover images. This means that the fidelity of the cover images are comparatively less interfered with resulting to higher levels of imperceptibility.

The MSE results are summarized below.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	0.87	2.26	Payload too big	Payload too big	Payload too big	Payload too big	Payload too big	Payload too big
Proposed LSB	0.40	1.66	Payload too big	Payload too big	Payload too big	Payload too big	Payload too big	Payload too big

TABLE 4: MSE Benchmark Results for The First Cover Image.

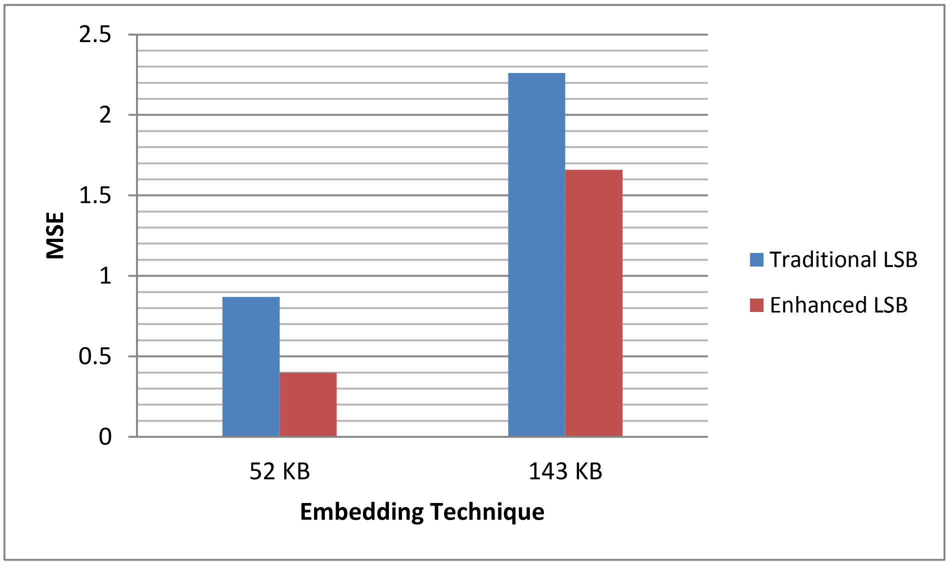


FIGURE 6: MSE Analysis for First Cover Image.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	0.15	0.41	0.71	1.15	1.28	1.67	1.80	2.18
Proposed LSB	0.06	0.21	0.41	0.77	0.9	1.28	1.42	1.86

TABLE 5: MSE Benchmark Results for The Second Cover Image.

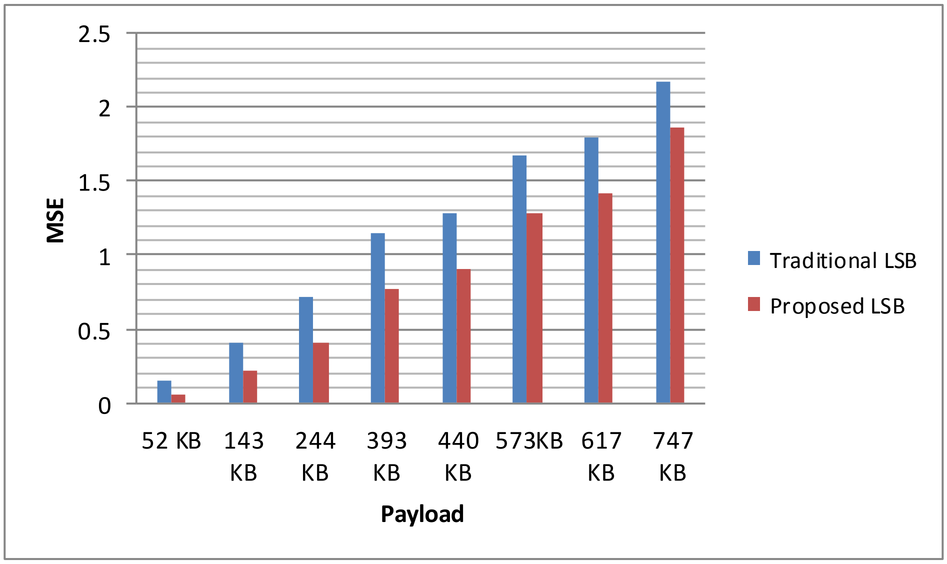


FIGURE 7: MSE Analysis for Second Cover Image.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	0.15	0.41	0.71	1.15	1.28	1.67	1.80	2.18
Proposed LSB	0.06	0.21	0.41	0.77	0.9	1.28	1.42	1.86

TABLE 6: MSE Benchmark Results for The Third Cover Image.

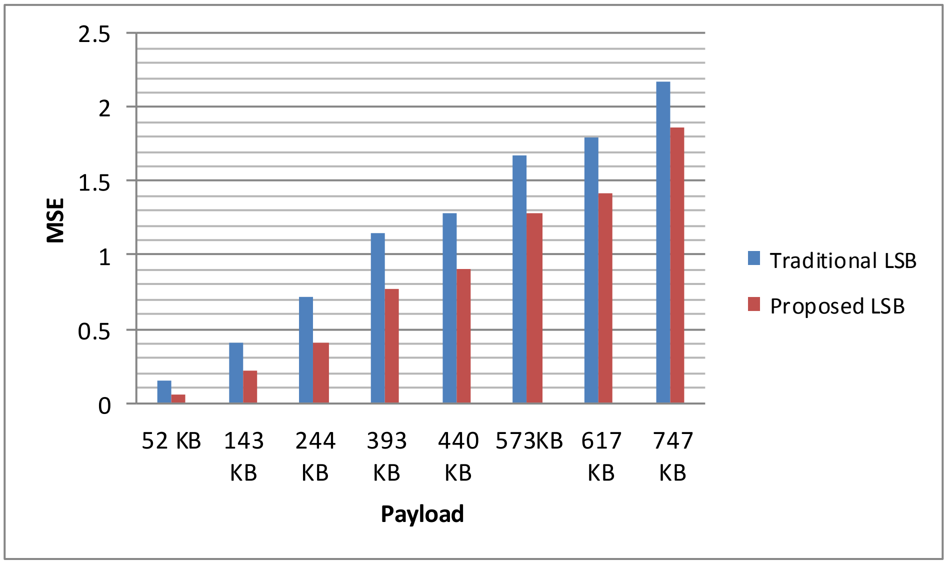


FIGURE 8: MSE Analysis for Third cover Image.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	0.107	0.292	0.500	0.804	0.900	1.173	1.265	1.530
Proposed LSB	0.04	0.14	0.27	0.49	0.57	0.80	0.88	1.14

TABLE 7: MSE Benchmark Results for The Fourth Cover Image.

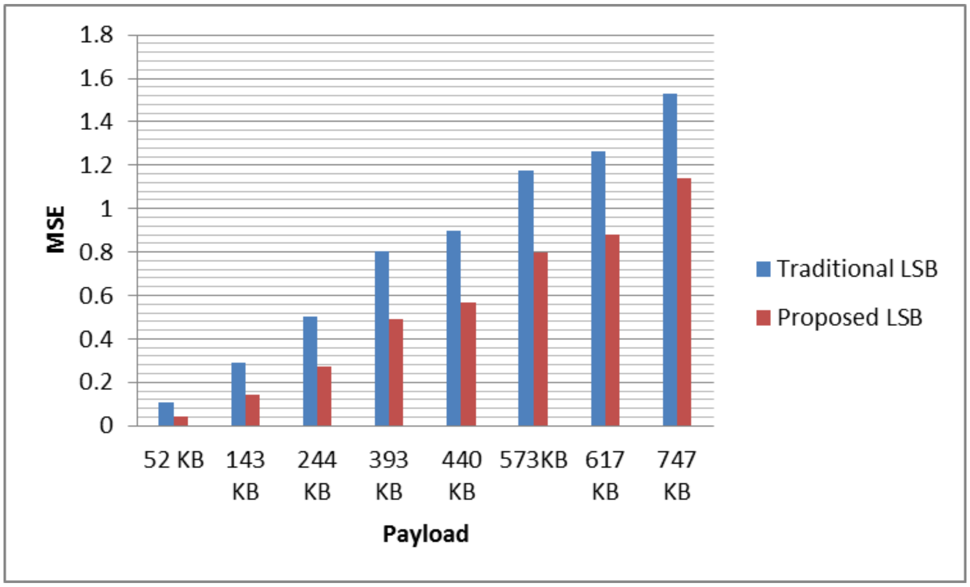


FIGURE 9: MSE Analysis for Fourth Cover Image.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	0.176	0.476	0.804	1.300	1.447	1.883	2.024	2.456
Proposed LSB	0.07	0.24	0.47	0.89	1.04	1.50	1.67	2.20

TABLE 8: MSE Benchmark Results for The Fifth Cover Image.

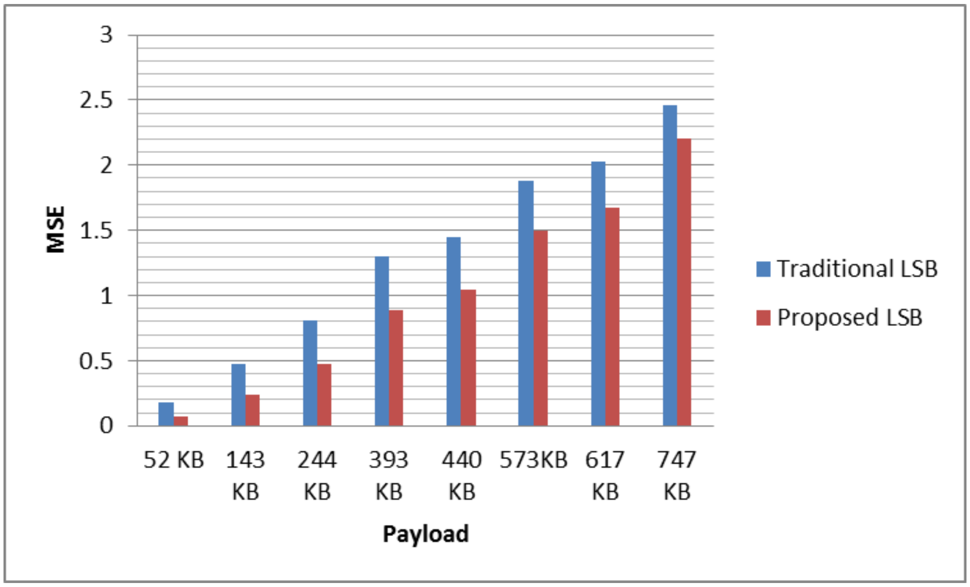


FIGURE 10: MSE Analysis for Fifth Cover Image.

Equally for all the payloads embedded in the five cover images, the proposed method posted higher levels of PSNR indicating that comparatively, less noise was introduced to the original cover images when the proposed method used. This helps in retaining the fidelity of the cover images and thereby enhancing imperceptibility. The PSNR results for the five images with different payloads are summarized below.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	58.23	54.12	Payload too big	Payload too big	Payload too big	Payload too big	Payload too big	Payload too big
Proposed LSB	61.55	55.45	Payload too big	Payload too big	Payload too big	Payload too big	Payload too big	Payload too big

TABLE 9: PSNR Benchmark Results for The First Cover Image.

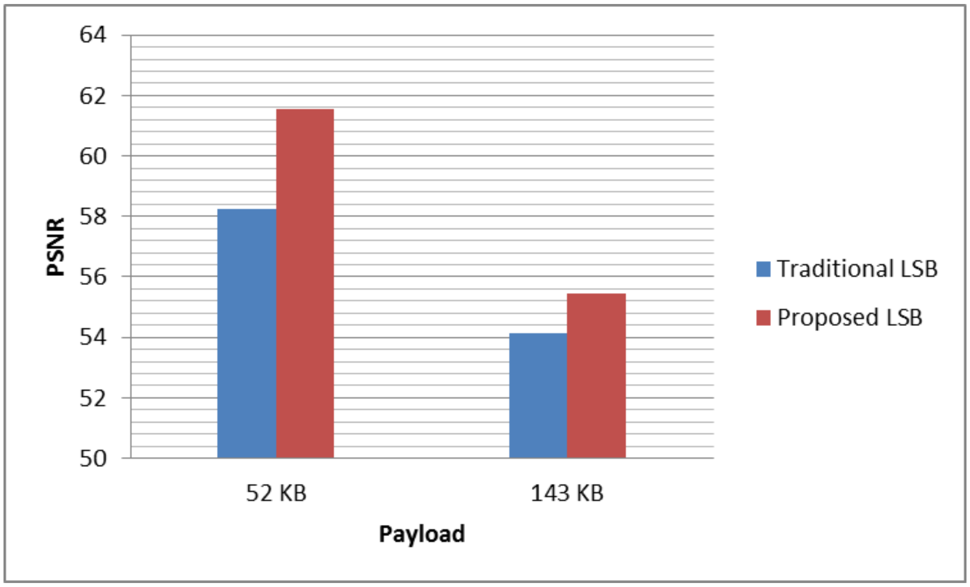


FIGURE 11: PSNR Analysis for First Cover Image.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	65.75	61.44	59.11	57.05	56.56	55.42	55.10	54.27
Proposed LSB	69.39	64.29	61.49	58.78	58.13	56.58	56.13	54.97

TABLE 10: PSNR Benchmark Results for The Second Cover Image.

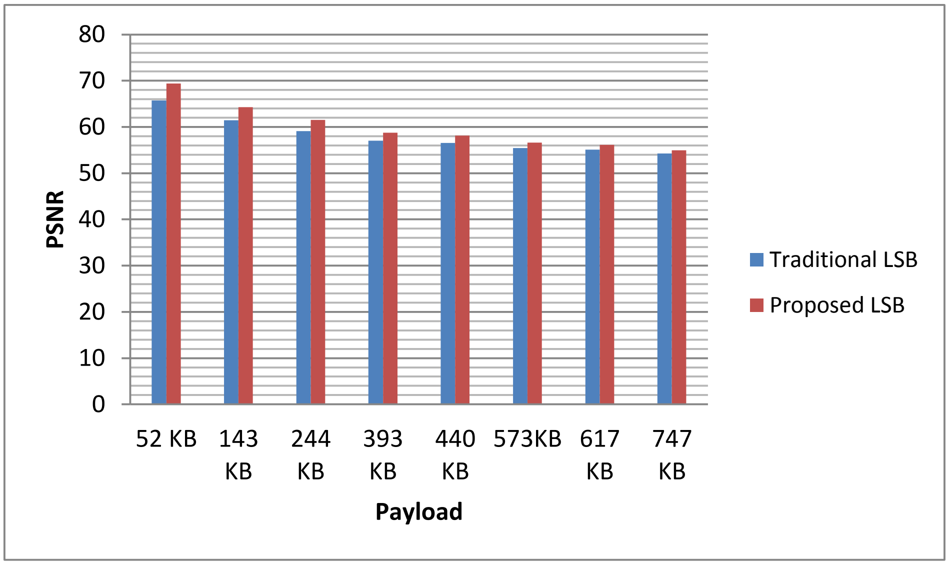


FIGURE 12: PSNR Analysis for Second Cover Image.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	65.87	61.45	59.14	57.07	56.57	55.43	55.11	54.27
Proposed LSB	69.39	64.28	61.49	58.78	58.13	56.58	56.13	54.96

TABLE 21: PSNR Benchmark Results for The Third Cover Image.

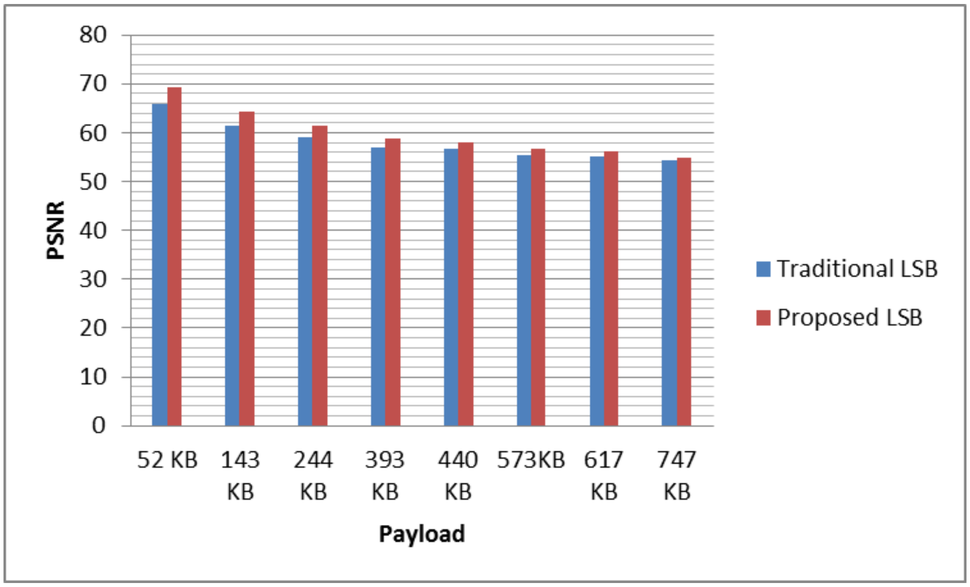


FIGURE 13: PSNR Analysis for Third Cover Image.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	67.37	63.01	60.68	58.61	58.12	56.97	56.64	55.82
Proposed LSB	71.00	65.98	63.28	60.70	60.07	58.61	58.19	57.09

TABLE 32: PSNR Benchmark Results for The Fourth Cover Image.

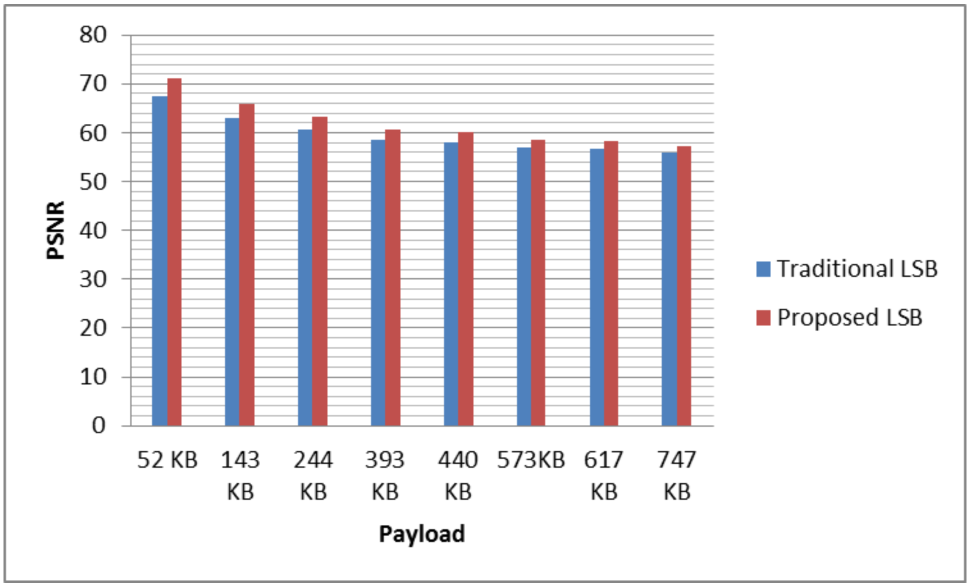


FIGURE 14: PSNR Analysis for Fourth Cover Image.

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	65.20	60.88	58.61	56.53	56.06	54.92	54.60	53.76
Proposed LSB	68.88	63.73	60.89	58.14	57.47	55.89	55.43	54.24

TABLE 43: PSNR Benchmark Results for The Fifth Cover Image.

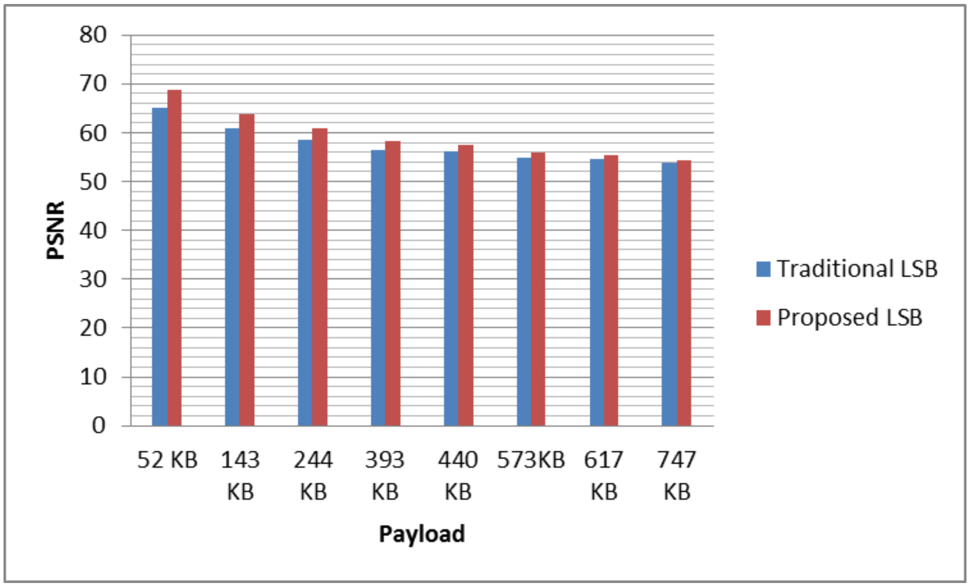


FIGURE 14: PSNR Analysis for Fifth Cover Image.

6. CONCLUSION

This research set out to investigate on an enhanced LSB steganographic method that can be used in improving the security in web based tele radiology systems. The impact of using the image's randomly targeted bits in the LSB steganography method embedding process on imperceptibility and detectability of hidden data was demonstrated and tested. The test results for the image metrics showed that using this technique for image bits swapping during the embedding process significantly improves on the imperceptibility and the detectability of the hidden data thereby ensuring better security of the MI transmitted through a web based tele radiology infrastructure. The experiment results also revealed that the proposed embedding method results in stego images of higher fidelity compared to the ones generated by the traditional method. Ensuring that the statistical characteristics of the original cover file are preserved as much as possible is the key to an effective steganographic method as this ensures the security of the embedded data against steganalysis. Embedding the EPHI as a watermark in the frequency domain of the cover image helps the remote radiologist to detect tampering on the MI thereby enforcing nonrepudiation which a key objective in web based tele radiology.

7. REFERENCES

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

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

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

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

[5] Kalaivanan., Ananth. and Manikandan. "A Survey on Digital Image Steganography", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 2015,

[6] Hemang A . Prajapati1, Dr. Nehal G. Chitaliya," Secured and Robust Dual Image Steganography: A Survey", International Journal of Innovative Research in Computer and Communication Engineering 2015

[7] Sedighi, V., Fridrich, J., & Cogranne, R. "Toss that BOSSbase, Alice!. Electronic Imaging, 2016 (8), 1-9.

[8] Bender, W. 'Techniques for Data Hiding', IBM Systems Journal, 35(3&4), pp 313-336.1996

[9] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux."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.

[10] C. Cachin." An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318.2008

[11] Neil, F. J. and Jajodia, S. "Exploring Steganography: Seeing the Unseen', IEEE Computer, 31(2), pp 26-34.1998.

[12] 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, pp. 1-12, 2012

[13] Krenn, J.R., "Steganography and Steganalysis". Accessed on 2nd March 2018. Available on http://www.krenn.nl/univ/cry/steg/article.pdf

[14] Steganalysis: Detecting LSB Steganographic Techniques T Sarkar, S Sanyal - arXiv preprint arXiv:1405.5119, 2014

[15] Cooper, Curtis . "Mersenne Prime Number discovery!". Mersenne Research, Inc. Retrieved 22 November 2016.

[16] Makoto Matsumoto and Takuji Nishimura. "Mersenne twister: a 623-dimensionally equidistributed uniform pseudorandom number generator" ACM Trans. on Modeling and Computer Simulation, vol. 8, no. 1, pp. 3-30, Jan. 1998.

[17] Makoto Matsumoto and Y. Kurita,."Twisted GFSR generators" ACM Trans. On Modeling and Computer Simulation, vol. 2, pp. 179-194, 1992.

[18] Makoto Matsumoto and Takuji Nishimura, "Dynamic Creation of Pseudorandom Number Generators", Monte Carlo and Quasi-Monte Carlo Methods 1998, Springer, 2000, pp 56—69.

[19] Archana Jagannatam. " Mersenne Twister – A Pseudo Random Number Generator and its Variants. ACM Transactions on Mathematical Software, 32(1):1–16.2013.

[20] Mutsuo Saito and Makoto Matsumoto, "SIMD-oriented Fast Mersenne Twister: a 128-bit Pseudorandom Number Generator", Monte Carlo and Quasi-Monte Carlo Methods, Springer, 2008, pp. 607 – 622.

[21] Sravanthi, G.S.; Mrs.B.Sunitha Devi, S.M.Riyazoddin& M.Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of Computer Science and Technology Graphics & Vision, Volume 12 Issue 15 Version 1.0. 2012.

[22] Prabhishek Singh, R S Chadha. "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT). pp 683-689. 2013.

[23] Iivari, J. and Venable, J. Action research and design science research – seemingly similar but decisively similar, In Proceedings to the 17th European Conference on Information Systems, Verona. http://www.ecis2009.it/papers/ecis2009-0424.pdf, accessed on September 14th 2014.

[24] Vaishnavi, V. and Kuechler, W." Design Science Research in Information Systems. DESRIST.org. Available at: http://desrist.org/desrist. Accessed on October 26th ,2016

[25] Kuechler, B., & Vaishnavi, V."The emergence of design research in information systems in north america. Journal of Design Research, 7(1), 1-16.2008

[26] Alturki, Ahmad and Gable, Guy G., "THEORIZING IN DESIGN SCIENCE RESEARCH: AN ABSTRACTION LAYERS FRAMEWORK" (2014). PACIS 2014 Proceedings. Paper 126.http://aisel.aisnet.org/pacis2014/126 accessed on December 17th 2017

[27] Betsy Samuel1, Vidya N.2." Wavelet Based Watermarking Approach of Hiding Patient Information in Medical Image for Medical Image Authentication". International Journal of Modern Trends in Engineering and Research. PP 453-458, 2015

[28] Kumar Ravi and Rattan Munish,." International Journal of Advanced Research in Computer Science and Software Engineering." Volume 2, Issue 11. Pp 137-134, 2012

[29] Kavitha S.and Thyagharajan K. K,." A Survey on Quantitative Metrics for Assessing the Quality of Fused Medical Images. Research Journal of Applied Sciences, Engineering and Technology 12(3): 282-293, 2016

[30] Kethepalli Mallikarjuna, Kodati Satya Prasad and Makam Venkata Subramanyam. ." Image Compression and Reconstruction using Discrete Rajan Transform Based Spectral Sparsing". Image, Graphics and Signal Processing, 2016, 1, 59-67

[31] Wang, Z. and Q. Li,. "Information content weighting for perceptual image quality assessment". IEEE T. Image Process., 20(5): 1185-1198. 2011

[32] Yusnita Yusof and Othman O. Khalifa, . "Digital Watermarking For Digital Images Using Wavelet Transform. Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, pp.14-17, 2007

[33] Wang, Z., Sheikh, H. R. & Bovik, A. C. "Non- reference perceptual quality assessment of JPEG compressed images. Proceedings of the International Conference on Image Processing, 1, 477-480. 2002

[34] MEMON FARIDA , MUKHTIAR ALI UNAR, AND SHEERAZ MEMON." Image Quality Assessment for Performance Evaluation of Focus Measure Operators". Mehran University Research Journal of Engineering & Technology, Volume 34, No. 4,pp 379-386, 2015

[35] Horé Alin and Ziou Djemel,." International Conference on Pattern Recognition." IEEE DOI 10.1109/ICPR. 2010, pp 2366-2369