The International Journal of Engineering and Science (IJES)
|| Volume || 7 || Issue || 6 Ver. I || Pages || PP 34-46 || 2018 ||
ISSN (e): 2319 – 1813 ISSN (p): 23-19 – 1805

Towards A More Secure Least Significant Bit (LSB) Steganographic Method for Information Hiding

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

[1]. Department of Information Technology,Dedan Kimathi University of Technology
[2&3] Department of Computing, Jomom Kenyatta University of Agriculture and Technology
Corresponding Author: Gabriel Kamau

--***ABSTRACT***--

Although the LSB algorithm for information hiding exploits the weakness of the human vision sensitivity (HVS) to hide secret data in a cover medium, it is relatively vulnerable to statistical steganalysis thus increasing the possibility of an eavesdropper decoding and retrieving the hidden message. This is partly aided by the sequential nature in which the algorithm replaces the target least significant bits of the cover image with the bits of the secret message making it easy for a steganalysis tool to zero in the image bits which are out of pattern with the rest.

To enhance the conventional LSB algorithm imperceptibility to steganalysis attacks, an embedding procedure that utilizes the Mersenne Twister (MT) pseudo-random number generator (PRNG) to help in spreading the secret data bits over the cover image in a non-sequential manner is proposed. Using the MT PRNG makes sure that the generated sequence of numbers is repeatable, has known mathematical properties and can be implemented without needing any specialist hardware. The idea is to generate a group of random numbers of length equal to the secret message length. This series of numbers are then used to identify the target pixels color channel bits for the purpose of embedding the secret message bits. Though this approach slightly reduces the capacity of a cover image for equal payloads, it significantly increases the imperceptibility and the security of the hidden information which was the prime focus of this study.

KEYWORDS *– Steganalysis, Steganographic, imperceptibility, Embedding, Capacity.*

Date of Submission: 26-05-2018 Date of acceptance: 11-06-2018

I INTRODUCTION

Steganographic techniques, though relatively new in the area of computer data security have provided a secure alternative way of exchanging sensitive content across computer networks particularly in countries where other methods like cryptography have been outlawed. These techniques are used to conceal secret data in innocent looking containers such as digital images, audio and video files (Mohammad Fahmi et al., 2008) .The secret message is normally embedded in a cover medium known as a *stego* file to effect hidden communication in plain sight.

The traditional LSB method is an insertion technique that inserts the bits of the secret information in the least significant bits of the cover file effectively concealing an entire file in a carrier file for the purpose of transmitting the embedded file to a remote recipient. The recipient then decodes the data from his/her end. The concept behind the LSB method is to replace the least significant bit (LSB) of each color channel bits in each pixel of a cover image with the bits of the information to be hidden. It is premised on the fact that the least significant bit has a place value of 1 and modifying it would result in minimum change to the color of the pixel and by extension the entire image. Such a modification would then be imperceptible to a human eye.

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

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

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

Increasing payload in LSB method significantly affects imperceptibility of the hidden information. Embedding capacity was defined by Lin and Delp as “the size of information that can be hidden relative to the size of the cover file" (Lin and Delp, 1999). It is the amount of secret information that can be hidden in a cover image without compromising imperceptibility. A good steganographic algorithm should have high payload capacity without overly compromising on imperceptibility. According to (Marvel et al, 2012), maximizing capacity and robustness of a carrier file while at the same time ensuring that the hidden information is imperceptibly embedded is a real challenge that requires an accurate trade-off. Bender discusses this trade-off between capacity and robustness as the *data-hiding problem space* (Bender, 1996). He outlines that in order to achieve robustness, redundant encoding of the embedded data on the cover-medium must be performed, which in turn definitely compromises capacity. This is illustrated in Fig. 1 based on Fridrich's diagram for the data-hiding problem space, which depicts the mutually competitive nature of these parameters (Fridrich et al., 2000).

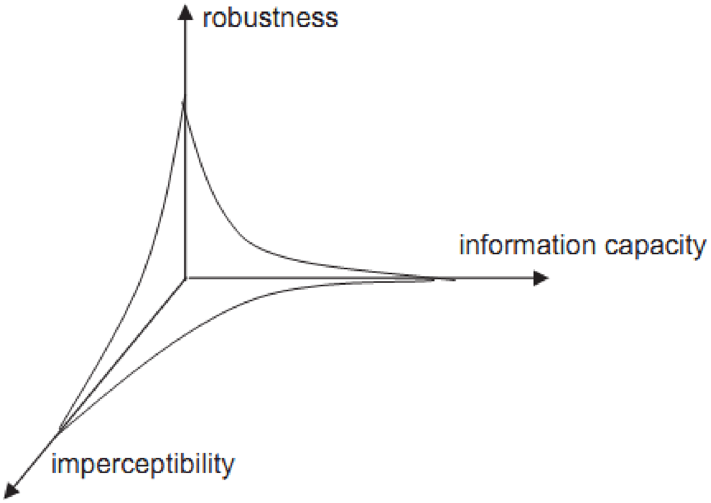


Figure 1: The Data-hiding problem space

To increase imperceptibility in the LSB insertion method for equal payload, this paper proposes the use of MT PRNG in choice of target image bits to swap with the secret data bits during the embedding process.

II PROPOSED METHOD

The proposed method employs a selective and randomized approach in picking target image bits in the carrier image using the MT PRNG. The selected carrier image bits are then swapped with the secret data bits to effectively embed the information in the carrier image.

2.1 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 (Makoto Matsumoto and Takuji Nishimura ,1998). As of January 2016, 49 Marsenne primes are known including the largest known prime number 274,207,281 − 1 which is a Marsenne prime (Cooper and Curtis, 2016). It has a period of 2^19937-1.

2.2 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 (Makoto Matsumoto and Y. Kurita, 1992). 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 , $0 \leq r \leq w\text{-}1$
u is upper or leftmost bits
l is lower or rightmost bits

The concatenation of the xk, upper bits and xk+1 lower bits yields a w dimensional vector making it possible for the matrix A to be multiplied from right (Makoto Matsumoto and Takuji Nishimura ,2000). 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 (Archana Jagannatam, 2013).

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 (Mutsuo Saito and Makoto Matsumoto ,2008).

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,
$1 \leq m \leq n$
R is the separation point of one word, or the number of bits of the lower bitmask, $0 \leq r \leq w - 1$
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

Table 1 32-BIT MT 19937 Parameters

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

The feedback shift register is composed of 624, 32- bit length elements and a total of 19937 cells (Makoto Matsumoto and Takuji Nishimura, 2000). 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 }
    }
}
```

2.2 Embedding Procedure

The proposed embedding procedure follows the steps outlined below.

Input: An m x n cover Image (C) , Secret File (F)
Output : Stego image(S)
Algorithm: Steps
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 secret file bit embedded in a color channel bit, bitToWrite[x][y][channel][bit]
4. For all cover 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 secret data
10. Output stego image(S).

2.3 Extraction Procedure

The proposed extraction procedure follows the steps outlined below.
Input: Stego Image (S)
Output: Secret File (F)
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 color 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 color 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 secret File (F)
```

The general model framework adopted for the generation of the stego files is based on the Birgit Pfitzmann generic model shown in Fig.2.

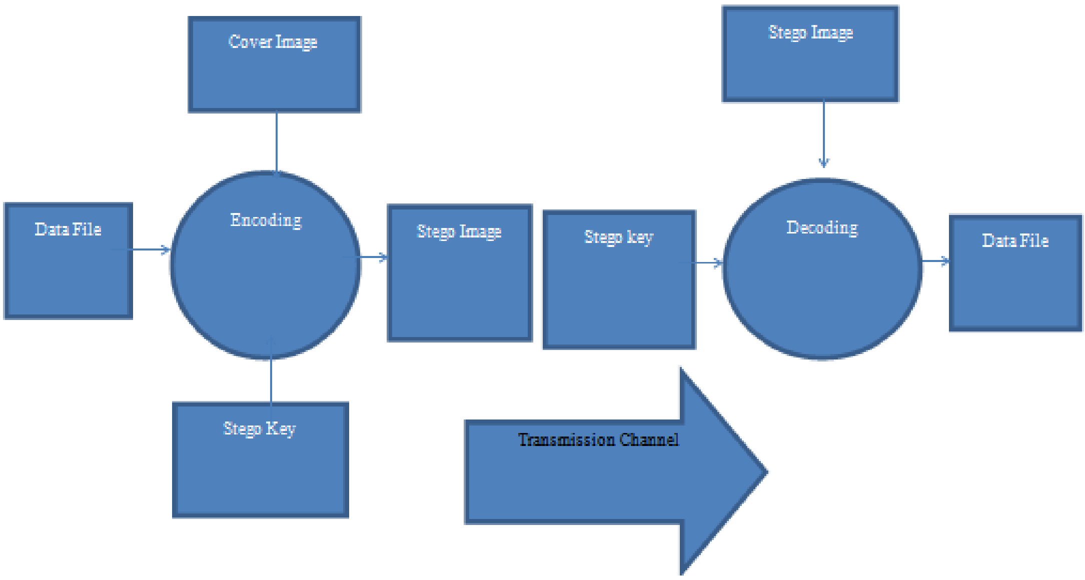


Figure 2: Model Framework

III EVALUATION AND DISCUSSION OF RESULTS

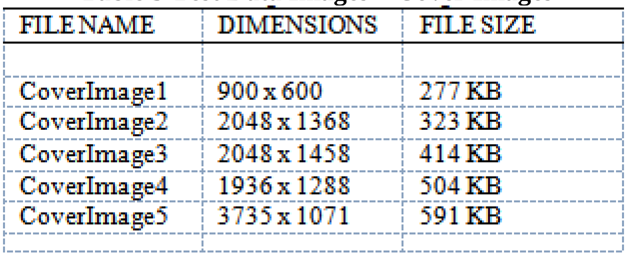
Eight MI payloads were used as test data files in five different cover files. The results were analyzed using the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) full reference image quality analysis metrics. Full reference image quality metrics are error sensitivity measures and are meant to establish the errors or image signal differences between the stego and the original cover images (Betsy and Vidya ,2015).

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 conventional LSB method and the proposed method.

Table 2 Test Data Images – Payloads (MI)

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 3
Image4.	1215 x 1041	393 KB	Payload 4
Image5	640 x 2237 P	440 KB	Payload 5
Image6	785 x 2001	573 KB	Payload 6
Image7	761 x 2412	617 KB	Payload 7
Image8	1079 x 194	747 KB	Payload 8

Table 3 Test Data Images – Cover Images



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

3.1 Mean Square Error (MSE)

MSE 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 (Kumar and Rattan, 2012). 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 (Kavitha and Thyagharajan ,2016). According to (Hemang et al.,2015), 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.

Lower readings of MSE in a stego image indicate closer similarity to the reference image (Kethepalli et al.,2016). The MSE for an image with a size of (M x N) is expressed as shown in Equation 3 (Wang. and Li, 2011).

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

Where:
Xij is the ith row and the jth column pixel in the original reference image,
Xij is the ith row and the jth column pixel in the reconstructed (stego) image,
M and N are the height and the width of the image,

MSE for color images is however defined differently as shown in equation (4) below (Wang et al., 2002).

$$MSE_{AVG} = \frac{MSE_{R} + MSE_{G} + MSE_{B}}{3} \qquad (4)$$

Where:

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

According to (Memon et al., 2015), 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.

3.2 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 (Horé and Ziou, 2010). It is one of the most extensively used metric parameter for the measurement of the quality of a reconstructed image (Memon et al., 2015). 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 (Horé and Ziou, 2010). The value of PSNR is computed using Equation (5)

$$PSNR = 10.\log 10 \frac{I^2}{(MSE)} db \qquad (5)$$

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.

3.3 MSE Metrics Bench mark results

Eight different payloads were embedded in five different cover images outlined in table 1 and table 2 using both the traditional LSB method and the proposed ELSB. For every test, stego images from the proposed method recorded slightly improved MSE ratios, indicating that comparatively less distortion is introduced to the original cover images using the proposed method. This means that the fidelity of the cover images for the ELSB method is relatively better resulting to higher levels of imperceptibility. These results are summarized in figures below.

Table 4: MSE benchmark results for the first Cover Image

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	,,	,,	,,	,,	,,
Proposed LSB	0.40	1.66	Payload too big	,,	,,	,,	,,	,,

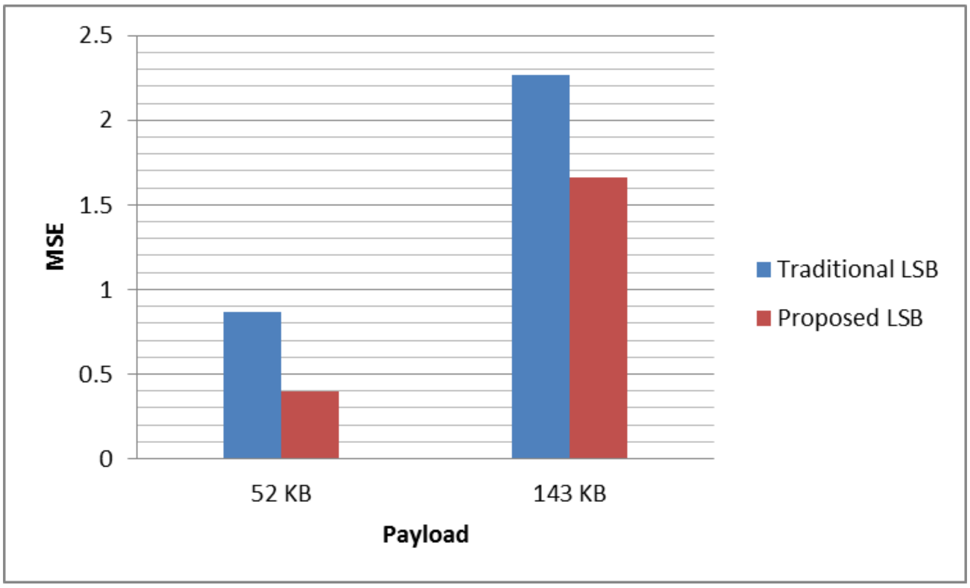


Figure 3: MSE first cover Image

Table 5: MSE benchmark results for the 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	0.90	1.28	1.42	1.86

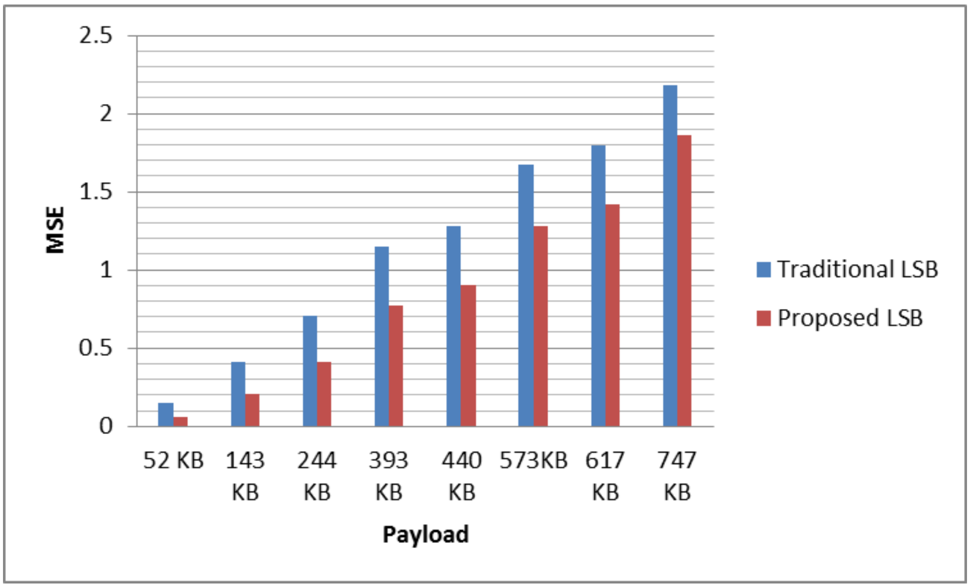


Figure 4: MSE second cover Image

Table 6: MSE benchmark results for the third 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	1.14	1.28	1.67	1.80	2.18
Proposed LSB	0.06	0.21	0.41	0.77	0.90	1.28	1.42	1.86

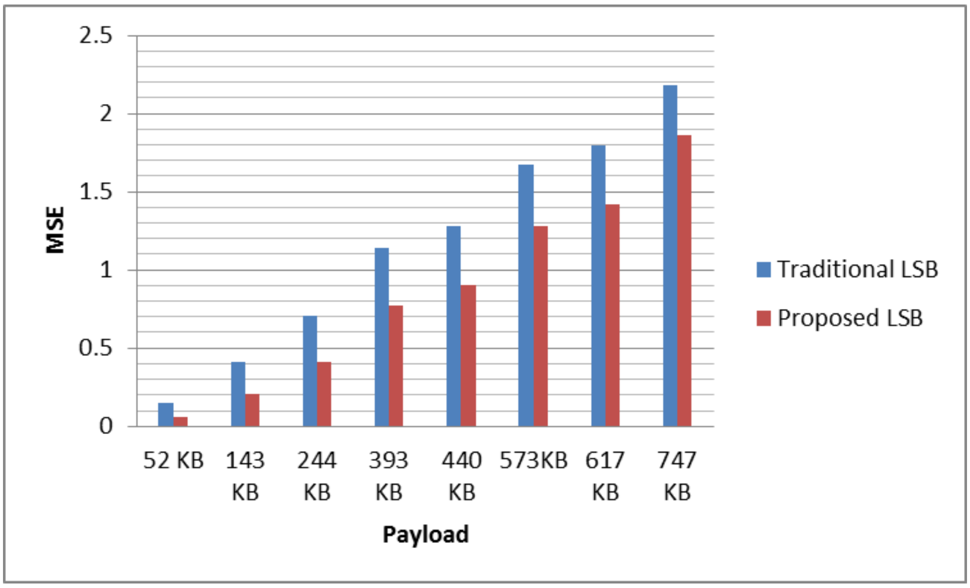


Figure 5: MSE third cover Image

Table 7: MSE benchmark results for the fourth Cover Image

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	0.10	0.29	0.50	0.80	0.90	1.17	1.26	1.53
Proposed LSB	0.04	0.14	0.27	0.49	0.57	0.80	0.88	1.14

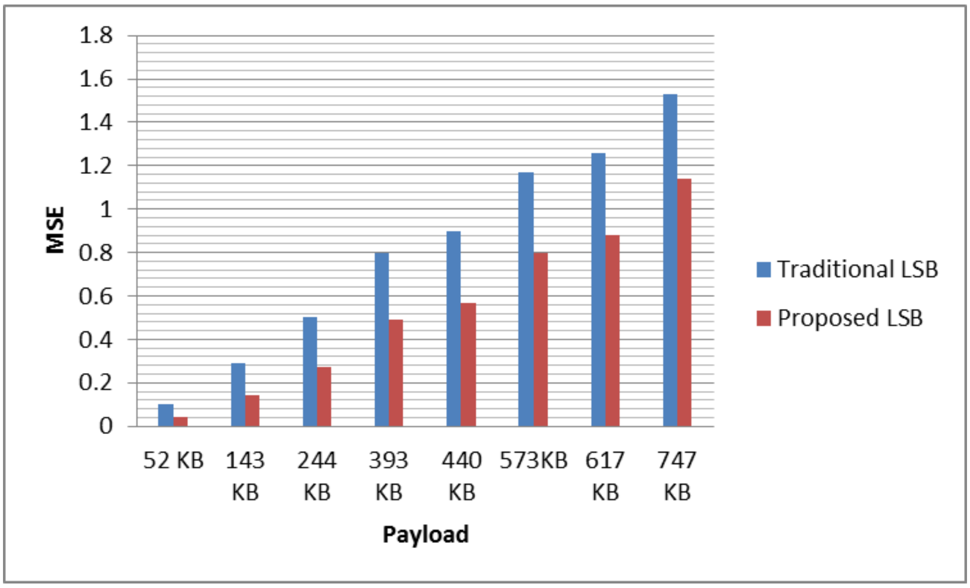


Figure 6: MSE fourth cover Image

Table 8: MSE benchmark results for the fifth Cover Image

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	0.17	0.47	0.80	1.30	1.44	1.88	2.02	2.45
Proposed LSB	0.07	0.24	0.47	0.89	1.04	1.50	1.67	2.20

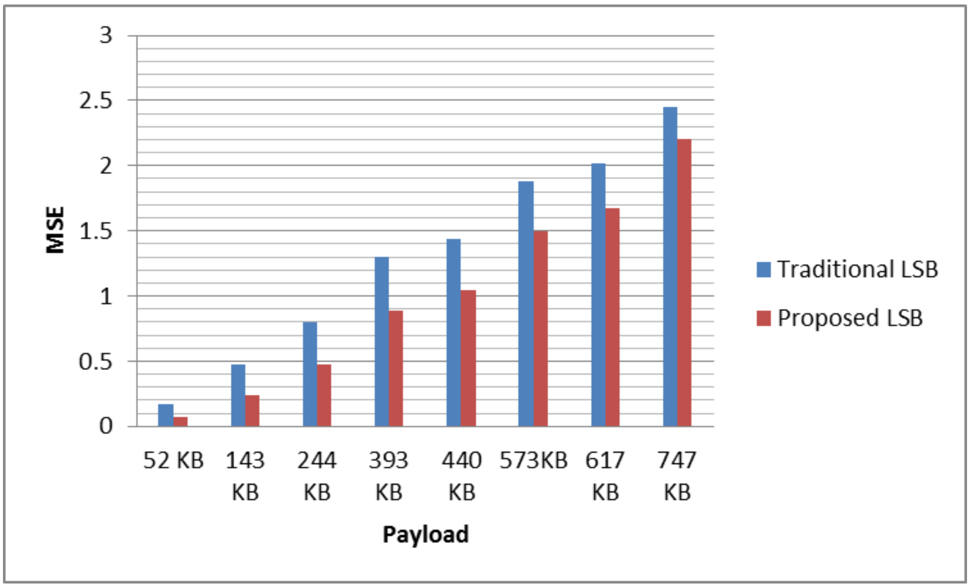


Figure 7: MSE fifth cover Image

3.4 PSNR Metrics Bench mark results

For all the payloads embedded in the five cover images, the proposed method posted higher levels of PSNR indicating comparative less noise as a result of embedding information in the cover images. This helps in retaining the fidelity of the cover images thereby enhancing imperceptibility.

Table 9: PSNR benchmark results for the first Cover Image

Technique	52 KB	143 KB	244 KB	393 KB	440 KB	573KB	617 KB	747 KB
Traditional LSB	58.223	54.12	Payload too big	,,	,,	,,	,,	,,
Proposed LSB	61.55	55.45	Payload too big	,,	,,	,,	,,	,,

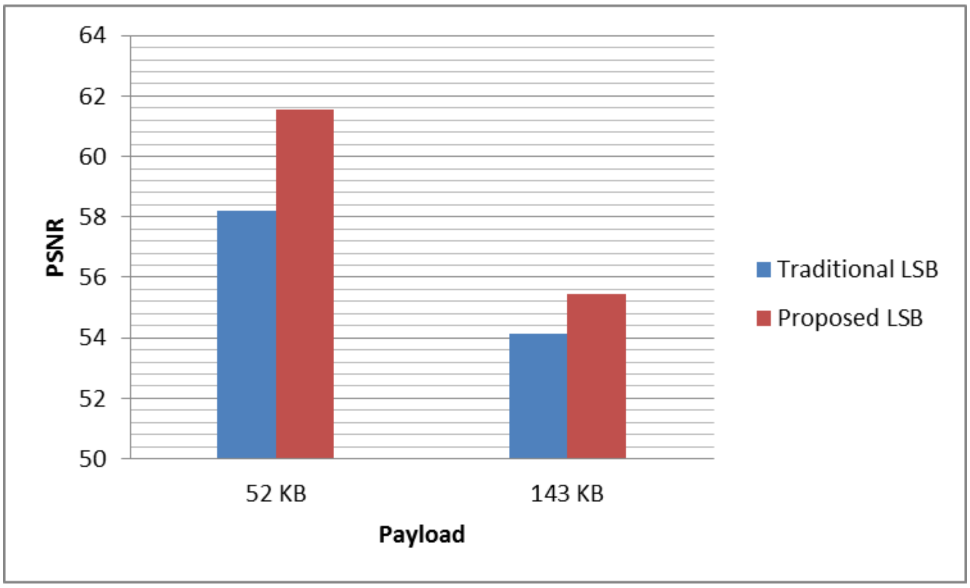


Figure 8: PSNR first cover Image

Table 10: PSNR benchmark results for the second 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

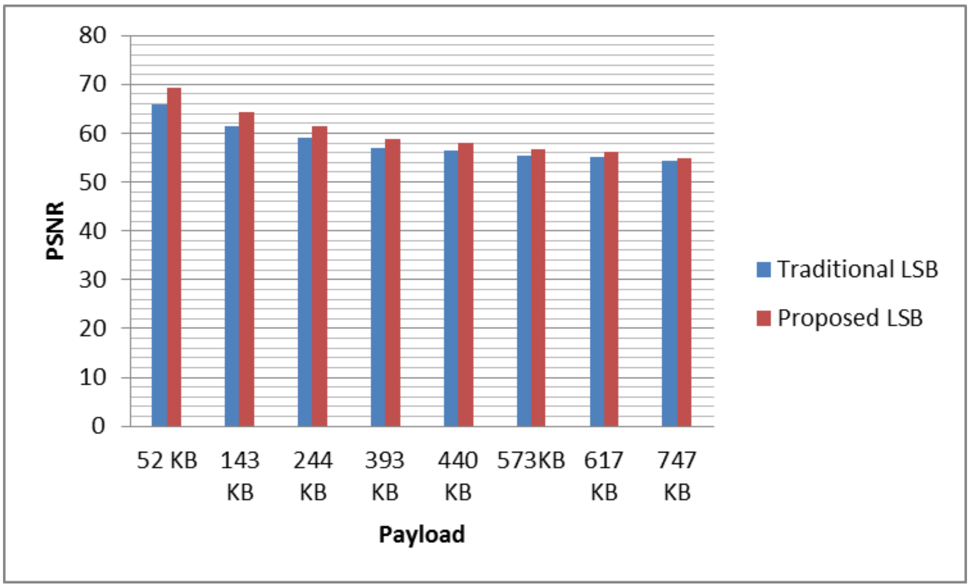


Figure 9: PSNR second cover Image

Table 11: PSNR benchmark results for the third 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	56.14	54.96

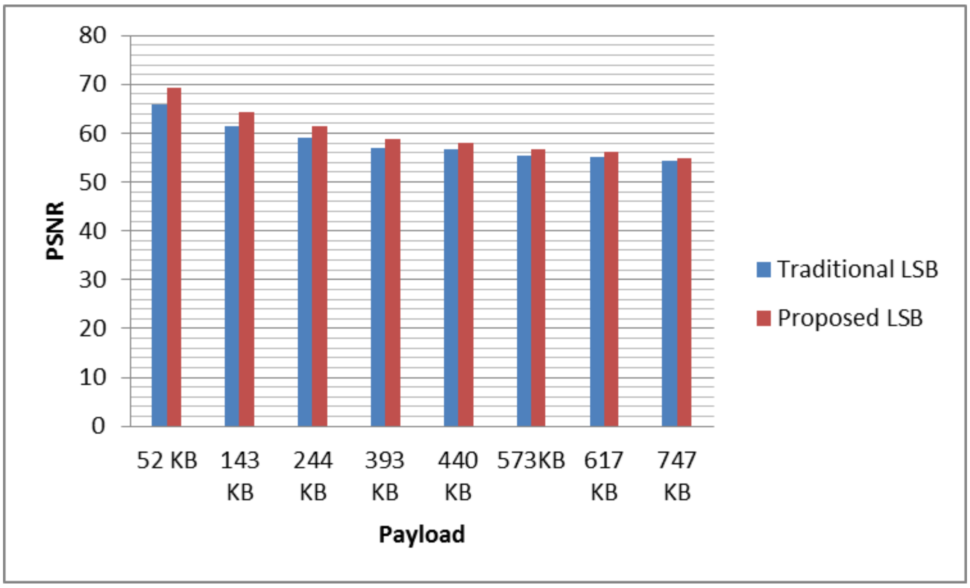


Figure 10: PSNR third cover Image

Table 12: PSNR benchmark results for the fourth 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	56.14	55.82
Proposed LSB	71.00	65.98	63.28	60.70	60.07	58.61	58.19	57.09

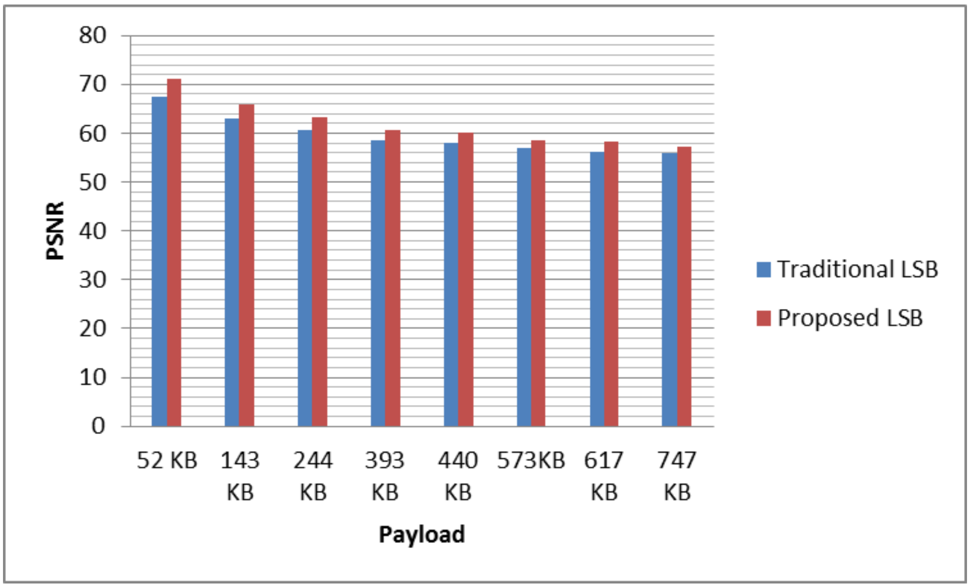


Figure 11: PSNR fourth cover Image

Table 13: PSNR benchmark results for the fifth 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	56.05	54.92	54.60	53.76
Proposed LSB	68.88	63.73	60.89	58.14	57.47	55.89	55.43	54.24

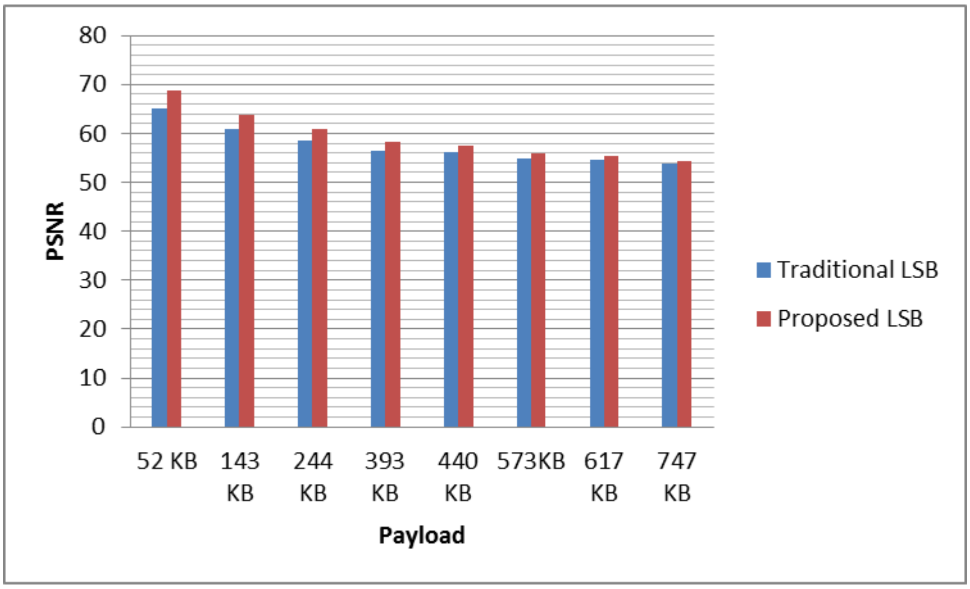


Figure 12: PSNR fourth cover Image

IV CONCLUSION

This research set out to investigate on an enhancing the security of the conventional LSB steganographic method. The impact of using MT pseudo random number generator to randomly target specific bits in the cover image during the embedding process was tested and demonstrated. 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 hidden information.

The analysis of the statistical differences as demonstrated using the two 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 in statistical imperceptibility of the hidden data. However, significant increase in payload seemed to slowly begin to have impact in signal distortion for the proposed method. However this can be mitigated by increasing the number of least significant bits used to two or even three.

REFERENCES

[1]. Archana Jagannatam (2013). Mersenne Twister – A Pseudo Random Number Generator and its Variants. ACM Transactions on Mathematical Software, 32(1):1–16.

[2]. Bender, W. (1996). 'Techniques for Data Hiding', IBM Systems Journal, 35(3&4), pp 313-336

[3]. Betsy Samuel1, Vidya N, (2015)." 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

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

[5]. Fridrich, J., Goljan, M. and Hogea, D. (2000) Attacking the OutGuess. The ACM Workshop on Multimedia and Security.

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

[7]. Lin E. and Delp E. (1999). 'A Review of Data Hiding in Digital Images', Video and Image Processing Laboratory, School of Electrical and Computer Engineering, Purdue University

[8]. Makoto Matsumoto and Takuji Nishimura (1998)."Mersenne twister: a 623-dimensionally equidistributed"

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

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

[11]. Marvel, L.M., Boncelet, C.G. and Retter, C.T (2012). 'Spread Spectrum Image Steganography', IEEE Transactions on Image Processing, 8(8), pp 1075-1083.

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

[13]. Mohammad, F. and Abdallah, M. (2008). "A Steganographic Data Security Algorithm with Reduced Steganalysis Threat," Birzeit University, Birzeit.

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

[15]. Kavitha S.and Thyagharajan K. K,(2016)." 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

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

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

[18]. Wang, Z., Sheikh, H. R. & Bovik, A. C. (2002b) No- reference perceptual quality assessment of JPEG compressed images. Proceedings of the International Conference on Image Processing, 1, 477-480.

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

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

Biographies

Gabriel Kamau is a PhD student in the department of computing in Jomo Kenyatta University. He has a first degree in Computer Information Systems, Masters in Software Engineering and his research interest is in the fields of data security, information hiding and signal processing. He currently teaches in the IT department of Dedan Kimathi University

Professor Wilson Cheruiyot is a senior lecturer in the department of computing of Jomo Kenyatta university of Agriculture and technology. His research interest is in multimedia data retrieval, internet of things and digital image processing.

Professor Waweru Mwangi is a senior lecturer in the department of computing of Jomo Kenyatta university of Agriculture and technology. His research interest is in artificial intelligence and simulation and modeling.

Gabriel Kamau." Towards A More Secure Least Significant Bit (LSB) Steganographic Method For Information Hiding." The International Journal of Engineering and Science (IJES) 7.6 (2018): 34-46