Performance Analysis of IoT Security scheme employing an Integrated Approach of Cryptography and Steganography

Ria Das, ria.das@wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download 

Abstract

Internet of Things (IoT) refers to the next phase of information revolution whose context involves billions of smart devices and sensors interconnected to facilitate speedy information and data exchange under soft real time constraints. IoT extends the **'anywhere, anyhow, anytime'** computing and networking paradigm to **'anything, anyone and any service'**. In this paper, a security scheme in IoT is analyzed where a fused approach of cryptography and steganography have been adopted. Two different steganographic schemes; Variable Least Significant Bit Substitution (VLSBS) and Most Significant Bit- Least Significant Bit (MSB-LSB) Substitution are analyzed using an experimental 2^4 X 3 design (48 experiments). Further an extensive literature survey is conducted in the steganography domain, to get an idea about popular steganographic metrics widely employed nowadays. Some of these metrics such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) , Normalized Cross Correlation (NCC), Normalized Absolute Error (NAE), Average Difference (AD), Maximum Difference (MD), Structural Content (SC) etc have been analyzed for the aforesaid steganographic schemes for the purpose of comparative performance analysis. Further, it has been verified that the number of cover image pixels required for data embedding as well as number of altered cover image pixels is less in case of MSB-LSB scheme that implies its better performance as compared to its VLSBS counterpart.

Keywords. Internet of Things (IoT), Steganography, Cryptography, Variable Least Significant Bit Substitution (VLSBS), Most Significant Bit - Least Significant Bit (MSB-LSB) Substitution, Data Encryption Standard (DES), Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Normalized Cross Correlation (NCC), Normalized Absolute Error (NAE), Average Difference (AD), Maximum Difference (MD), Structural Content (SC), Structural Similarity Index (SSIM).

Contents

1. Introduction

The Internet has transformed into Internet of Things (IoT) propelled by the ever increasing and spectacular advancements conducted in the domain of mobile communications and wireless technologies. IoT refers to the next phase of information revolution whose context involves billions of smart devices and sensors interconnected to facilitate speedy information and data exchange under real time constraints. The phrase 'Things' refer to the inseperable mixture of hardware,software, data and services. IoT extends the 'anywhere, anyhow, anytime' computing and networking paradigm to 'anything, anyone and any service'. However, since IoT typically involves multitude of constrained devices i.e sensors with limited computing power, battery life, memory, storage constraints, it is highly vulnerable to attacks. Thus ensuring data security during information exchange phase is of paramount importance in IoT.

In this paper, two proposed security schemes in IoT are analyzed employing a merged approach

of Cryptography and Steganography schemes mentioned in papers [Das17-Das16]. The goal here is to evaluate and examine the performance of the proposed security steganograhic schemes using various popular steganographic and performance metrics.

Cryptography refers to the science of attaining security by encrypting messages to make them non-readable. The process of converting from the plaintext (original data) to ciphertext (coded data) is known as encryption while the reverse process is termed as ***decryption***. If the ***same key*** is utilized for both encryption and decryption then the cryptographic model is termed a ***Symmetric Cryptography*** model else ***Asymmetric Cryptography***. In IoT lightweight Cryptography is desirable since IoT devices are constrained devices and lightweight schemes provide high efficiency for end-to- end communications as well as can be applied on low resource devices.

Steganography, on the other hand, refers to 'covered or hidden writing'. The goal of this scheme is to hide the very existence of the message/data in a cover medium. Modern steganographic schemes employ various cover mediums like the audio, image,video, network/protocols etc to embed data securely and then transmit it over the network. Applications of Steganography exist primarily in secret communications, feature tagging, copyright protection etc.

Eavesdropping is a very typical attack which is highly likely in IoT environment. One such scenario has been depicted in the Fig.1 below. It displays the data flow in the system under investigation. Firstly, the sensor captures the data which is transferred to an Authentication Server/Home Server for authentication purpose. Next, the data is migrated to the Clouds for further computation and analysis as per the requirements of deployed IoT applications. As shown the transferred data can be subjected to an eavesdropping attack. To address the aforesaid issue, an interesting model has been undertaken. A combined approach of Cryptography and Steganography scheme can be adopted to ensure data confidentiality and integrity. The implementation of the adopted scheme is next discussed briefly.

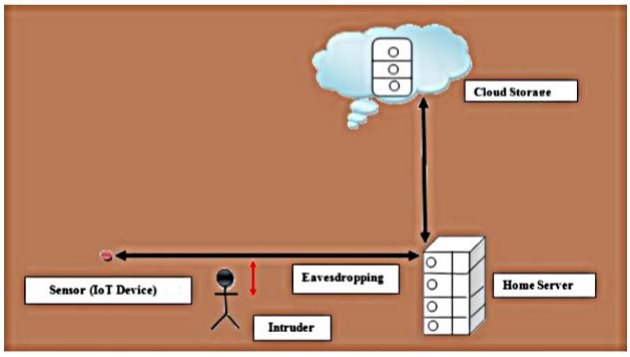

Fig.1. IoT Scenario [Das16]

The two steganographic algorithms which are undertaken for analysis in the aforementioned model consists of ***Variable Least Significant Bit Substitution scheme (VLSBS) [Das17] and Most Significant Bit- Least Significant Bit Substitution schemes (MSB-LSB) algorithms[Das16]***. The detailed model description is next highlighted.

The stepwise implementation of adopted security scheme is presented below:

- **Step 1: Sensor (IoT device site)**

    - The sensor data is first encrypted using a lightweight encryption scheme (XOR between sensor data and XOR key).
    - The message digest of the sensor data is computed using MD5 (Message Digest 5) algorithm.
    - Finally the encrypted data, computed digest and encryption key is embedded in a randomly selected cover image thereby producing the stego image using ***Simple Least Significant Bit Substitution scheme (SLSBS) of Steganography.***
- **Step 2: Sensor (Home Server site)**
    - Using reverse Steganography scheme, the encrypted data, encryption key and message digest is retrieved.
    - Using the retrieved encryption key the encrypted data is decrypted.
    - The message digest of the sensor data is recomputed using MD5 (Message Digest 5) algorithm.
    - Finally the newly computed digest is compared to the retrieved digest and both are compared to verify data integrity. If they are identical, then data integrity is assured to be preserved and authenticity is verified else data is discarded by home server.
- **Step 3: Home Server site**
    - Once again the sensor data is now encrypted using standard symmetric cryptographic scheme; Data Encryption Standard (DES).
    - The message digest of the sensor data is computed using MD5 (Message Digest 5) algorithm.
    - Finally the encrypted data, computed digest and secret key is embedded in a randomly selected cover image thereby producing the stego image using ***Variable Least Significant Bit Substitution scheme (VLSBS)*** of Steganography. Eventually the stego image is migrated to the clouds for further computation and analysis.

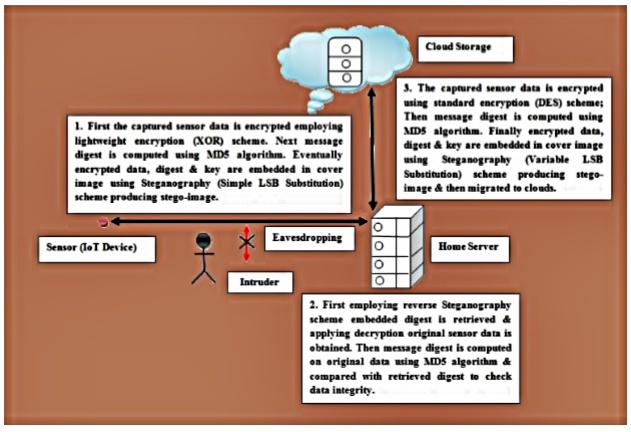

Fig.2. Proposed Security model in IoT adopting VLSBS scheme[Das17]
Fig.2. above depicts the approach discussed above. Besides another model can be implemented with a new steganographic algorithm; Most Significant Bit- Least Significant Bit Substitution (MSB-LSB) scheme [Das16] instead of Variable Least Significant Bit Substitution at home server site (step 3, last step) shown below in Fig.3.

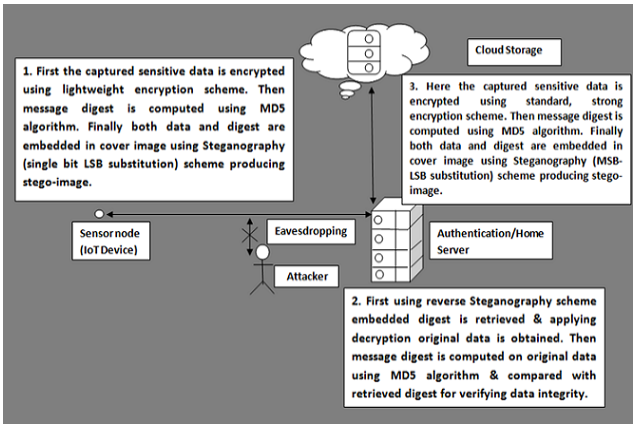

Fig.3. Proposed Security model in IoT adopting the MSB-LSB scheme [Das16]

In this paper, performance analysis is conducted for all the above implemented security schemes along with the computation of some popular steganographic performance metrics. An extensive literature survey is conducted in this domain the details of which are presented in the literature review section of this paper.

The structure for this paper is organized as follows. Section 2 highlights the literature survey conducted in the domain of Steganography highlighting some of the popular performance metrics. Section 3 puts forth overview of the proposed steganographic schemes: SLSBS, VLSBS and MSB-LSB schemes as adopted in papers [Das17-Das16]. Section 4 analyzes the computed performance metrics along with the experimental computations. Finally section 5 discusses the concluding section of this paper.

2. Literature Review

Already several researchers worldwide have worked in the domain of Cryptography and Steganography and thus have adopted various metrics for analyzing the performance of their proposed methodologies and schemes. In this section briefly, some of such existent works and the analyzed metrics have been put forth.

2.1. Image Steganography Combined with DES Encryption Pre-processing [Ren14]

Researchers Yang Rener et al., in this work, have adopted a merged approach of Cryptography (DES) and Steganography (LSB substitution scheme) so as to enhance the security of Steganographic algorithm. One of the inherent issues with Cryptography lies in the fact that even if data is encrypted, the encoded data still remains available in coded textual format that can easily arouse suspicion by attackers or malicious minds. However, with Steganography, the data gets embedded in a cover medium that intrinsically not only veils the secret data but also hides the fact that communication had occurred. Definitely, both these schemes complement and

reinforce each other thereby enhancing the security of the hidden and covert data communication.

Here a very simple approach is explored. The data to be hidden is first encrypted using DES and then both the encrypted data version and key are embedded in a cover image using LSB substitution scheme of Steganography at the sender site. On the receiver end, first using reverse Steganography the encrypted data and key are retrieved followed by the decryption of the data with the retrieved key.

For the purpose of evaluation of the undertaken Steganography scheme, the metrics which have been considered here include:

- **Histogram Difference and the Sum of Histogram Absolute Difference:**
  The difference between the histograms of cover image and stego image are compared so as to figure out the visible distortion (if any) between them. The absolute histogram difference expresses the degree of change visible both before and after applying Steganography.
- **Relative Entropy (K-L Divergence) of image (both before and after adoption of Steganography):**
  It is used to estimate the security of the undertaken steganographic scheme. The lower the value the better is the security offered by the scheme.

2.2. Comparative Analysis of Steganographic Algorithms Within Compressed Video Domain [Idb14]

Researchers Tarik Faraj Idbeea et.al have analyzed and compared three steganographic schemes namely i) Least significant bit insertion, ii) Bit plane complexity segmentation and iii) Enhanced version of pixel value difference (EPVD). The motivation for this work was attributed to minimal research focus of veiling data in compression domain for a class of video-based embedding methods. The work which is analyzed here involves examining the devised steganographic schemes which were primarily based on embedding secret information during the MPEG-2 compression process within the quantized AC-Coefficients of the video frames.

The performance metrics that were considered here includes the following:

- **Compression Ratio (CR):**
  It refers to the ratio of the number of bits of the original video to the number of bits used to represent the compressed video.
- **Mean Square Error (MSE):**
  It measures the difference between the reference and processed data signals. Large MSE value signifies poor quality of modified signal.
- **Peak Signal to Noise Ratio (PSNR):**
  This works primarily based on only the measurement of the power of distortion present in the processed signal to the information present in the reference signal. High PSNR value implies good quality of processed signal.

- **Structural Content (SC):**
  This metric estimates the similarity of the structure of two data signals. Its value range from 0 to 1. High SC value implies better match between compared signals.

2.3. Steganography in Arrhythmic Electrocardiogram Signal [Jer15]

Researchers S Edward Jero et.al. have put forth an interesting scheme of hiding medical patient data employing an abnormal Electrocardiogram (ECG) signal as the cover signal using Steganography technique. Precisely the medical information is embedded in a 2D ECG matrix of an arrhythmic ECG signal (obtained from MIT-BIH arrhythmia database).

The performance metrics for the aforementioned scheme are enlisted below:

- **Peak Signal to Noise Ratio (PSNR):**
  Transparency of patient data is computed here.
- **Percentage Residual Difference (PRD):**
  Difference between cover and stego signal id is estimated using this metric.
- **Kullback-Leibler distance (KL):**
  This metric estimates the probability difference between cover and stego signal id.
- **Bit Error Rate (BER):**
  The percentage of loss of data in the retrieved patient data is estimated using this metric.

2.4. A Cost Effective Approach for Securing Medical X-ray Images using Chebyshev Map [Red16]

Researchers V. Praneeth Kumar Reddy et.al. have adopted a novel and cost effective scheme for securing medical X-ray images employing a Chebyshev Map which employs chaotic maps. This hides the patient data confidentiality and increase the protection in medical images . Discrete and random numbers are generated here via the chaotic maps (Henon and Chebyshev maps) that are ultimately employed to assign the positions of the embedded information in the medical image. This approach gives the smaller key size and as the quantity of information to be inserted is less, the information loss is at minimum.

The performance metrics which have been analyzed in this work are briefly stated as follows:

- **Mean Square Error (MSE):**
  It estimates the cumulative square error between cover image and stego image.
- **Peak Signal to Noise Ratio (PSNR):**
  It depicts the noise content between cover and stego image.
- **Correlation Coefficient:**
  It measures similarity index between two i.e cover and stego image .

2.5. Local Binary Pattern Operator based Steganography in Wavelet Domain [Sin16]

Researchers Anuradha Singhal et.al. in this work have proposed a novel steganographic scheme based on Local Binary Pattern (LBP) operator in wavelet domain for embedding and retrieval of information. LBP operator examines the local intensity relationship of a coordinate with respect to its neighboring coordinates and can be used for both image retrieval and texture classification. LBP patterns are calculated by exploiting Boolean functions on frequency coefficients in wavelet domain and one or more pixels are adjusted in neighborhood to embed secret message. This scheme embeds data in the most suitable coefficients that not only maintains imperceptibility but also offers better security against data confidentiality attacks.

The performance metric that have been investigated here also includes the PSNR and SSIM metric which has been introduced below:

- **SSIM (Structural Similarity Index):**
  It considers image degeneration since perceived change in pixels has strong interdependencies specifically when images are spatially close and identical images. Its magnitude varies in range of -1 to 1 (value is 1 for identical images).

2.6. Performance Analysis of Digital Image Steganographic Algorithm [Jam14]

Researchers N.D. Jambhekar et.al. have analyzed the performance of Digital Image Steganographic Algorithms both in spatial and frequency domains. In the spatial domain, the analysis is conducted employing the spatial based methods carried out by the image pixel base using the techniques such as Least Significant Bit (LSB) insertion and spread spectrum methods. In the frequency based methods, the Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT), Discrete Fourier Transformation (DFT) and Integer Wavelet Transformation (IWT) steganographic transformation based methods are analyzed to hide secret image i.e. the payload to another cover image. The metrics which have been analyzed are enlisted below:

- **Peak Signal to Noise Ratio (PSNR):**
  It is defined as the ratio between the peak signal and alteration noise signals that affects the accuracy of its presentation of stego image.
- **Mean Squared Error (MSE):**
  The Mean Squared Error (MSE) is used to quantify the difference between actual values and estimated values.
- **Normalized Cross-Correlation (NCC):**
  Correlation is employed as an effective similarity measure in matching tasks. This

function returns the normalized cross correlation between the calling data series and the argument, the input data series.

- **Average Difference (AD):**
  This gives an estimation of the average difference between the selected pixel values of cover and stego images.
- **Structural Content (SC):**
  This measures the similarity between the cover and stego images by analyzing the count of the similar regions in both the images.
- **Normalized Absolute Error (NAE):**
  It refers to the statistical difference between the cover and stego image. A large value indicates a low quality while a small value indicates a high quality.

2.7. Steganography based information security with high embedding capacity [Sir15]

Researcher B. Lakshmi Sirisha et.al. have proposed a high embedding capacity for spatial domain image steganography in this work. By employing the (t, n) threshold secret sharing scheme, here two secret images are embedded in a cover image of same size with relatively high quality. In this approach, the secret image is communicated among n participants. Additionally, any t (or more) out of n authorized participants can only recover the secret image whereas less than t participants however cannot reconstruct the same.

The performance metrics used in this work includes the follows: **i) Peak Signal to Noise Ratio (PSNR) ii) Mean Squared Error (MSE) iii) Structural Similarity Index (SSIM) iv) Average Difference (AD) v) Normalized Cross-Correlation (NCC) vi) Normalized Absolute Error (NAE)** that have been already discussed in the previous papers.

2.8. 2L-DWTS - Steganography technique based on second level DWT [Bed16]

Researchers Punam Bedi et.al. have undertaken a steganographic technique here that is primarily based on Discrete Wavelet Transform (DWT) scheme. In this work a novel steganography technique 2L-DWTS is proposed, which applies discrete wavelet transform twice on the cover image and embeds the secret data or message in second level high frequency components. To retrieve the stego image, inverse DWT is employed on these components. Veiling the data in one of these high frequency components is not reflected since data spreads evenly across the stego image. Applying DWT twice appends an additional security layer specifically generating sixteen components which facilitates hiding four times stronger to susceptibility.

The performance metrics which have been analyzed in this work consists of the follows; **i) Peak Signal to Noise Ratio (PSNR) ii) Mean Squared Error (MSE) iii) Structural Content (SC) iv) Normalized Cross-Correlation (NCC) v) Normalized Absolute Error (NAE) and vi)**

Image Infidelity (IF). Most of these have been already discussed above.

Image Infidelity (IF) is computed when an accurate match is sought between the stego and cover image without having any visible distortion or loss of information.

2.9. Secret Data Transmission using Vital Image Steganography over Transposition Cipher [Jai15]

Researchers Mamta Jain et.al. in this work have performed secret data transmission employing vital image steganography scheme over transposition cipher. In this work, two varieties of security mechanism have been considered; cryptography and steganography. First, encryption is performed adopting Vernam cipher (One-Time Pad) transposition technique scheme. Next, cipher text is transformed into bytes and each byte divided into bit pairs and the decimal values are assigned to each pairs, which is termed as the master variable (Value of master variable varies between 0 to 3). Depending upon the master patchy value, the cipher text in the career image is added at Least Significant Bit (LSB) 6th and 7th bit location or 7th and 8th bit location or 7th and 6th or 8th and 7th bit locations. Eventually the cipher texts are retrieved from the said locations followed by the decryption process using the Vernam cipher (One-Time Pad) transposition algorithm.

The performance metrics that have been considered here are **i) Peak Signal to Noise Ratio (PSNR)** and **ii) Mean Squared Error (MSE)** which have been already described above.

2.10. Performance Evaluation Parameters of Image Steganography Techniques [Pra16]

Researchers Anita Pradhan et.al. have in this work highlighted some of the performance evaluation parameters of Image Steganography schemes. The performance of a steganographic technique can be rated by three parameters; i) hiding capacity, ii) distortion measure and iii) security. The hiding capacity refers to the maximum quantity of information that can be embedded in an image which is also represented as the number of bits per pixel. The distortion is measured by using various metrics like **i) Peak Signal to Noise Ratio (PSNR) ii) Mean Squared Error (MSE) iii) Structural Similarity Index (SSIM)**, Correlation etc all of which have been already highlighted in the previous works.

2.11. Performance Evaluation of Image Steganography Based on Cover Selection and Contourlet Transform [Sub13]

Researchers Mansi S. Subhedar et.al. in this work have presented a novel idea to hide secret data in contourlet domain. Here, the cover selection criteria is based on contrast measurement. Using contrast measurement, suitable cover is chosen from standard test image database and then embedding is carried out in contourlet sub bands of cover image.

The performance metrics that have been analyzed here includes the follows; **i) Peak Signal to Noise Ratio (PSNR) ii) Mean Squared Error (MSE) iii) Structural Similarity Index (SSIM)** all of which have been discussed earlier.

2.12. Objective Quality Metrics in Correlation with Subjective Quality Metrics for Steganography [Waz15]

Researchers Raniyah Wazirali et.al. have conducted a comparative study between objective quality metrics with subjective quality metrics in this work. Most of the ongoing studies employ the Peak Signal to Noise Ratio (PSNR) as a metric for imperceptibility evaluation, although it furnishes less accurate results as compared to the Human Visual System (HVS) evaluation. This paper provides a review of the existent evaluation metrics that are used to assess the quality of adopted steganographic scheme.

The performance metrics which have been adopted here includes; **i) Peak Signal to Noise Ratio (PSNR) ii) Mean Squared Error (MSE) and iii) Structural Similarity Index (SSIM)** all of which has been explicitly described earlier.

2.13. Enhanced Data Concealing Technique to Secure Medical Image in Telemedicine Applications [Val16]

Reserachers G. Vallathan et.al. have performed an enhanced data hiding scheme to secure medical image transference in telemedicine applications. In this paper, both encryption and steganography technique have been employed to improve the security of both patient's privacy information as well as the medical image. The host medical image undergoes Contourlet Transform to provide the innate geometrical structures of an image like curves instead of points and it offers the directionality and anisotropy property. Next, the patient privacy information is embedded over the high frequency components of a transformed image using LSB embedding algorithm. Finally the data concealed image is encrypted using LBG (Linde Buzo Gray) algorithm to ensure security.

The performance metrics which have been analyzed here comprises the follows; **i) Peak Signal to Noise Ratio (PSNR) ii) Mean Squared Error (MSE) and iii) Structural Similarity Index (SSIM)** all of which have been explicitly discussed above.

2.14. Stochastic Local Search Combined with LSB Technique for Image Steganography [Bou16]

Researchers Dalila Boughaci et.al. have proposed a novel steganographic methodology to hide a message in the image. The proposed technique adopts an integrated approach of Stochastic Local Search meta-heuristic (SLS) with the least significant bits method (LSB).The LSB approach was improved by combining it with the SLS technique. Here the researchers have adopted 3 methods LSB (Least Significant Bit), LSB + LS (local search) and LSB+ SLS (stochastic local search) and evaluated all on some series of JPEG images.

The performance metrics which have been analyzed here comprises the follows; **i) Peak Signal to Noise Ratio (PSNR) ii) Mean Squared Error (MSE) and iii) the Encoding Time all proposed schemes.**

Thus, in this section, a detailed literature survey has been furnished that gives idea about some of the widely employed steganographic performance metrics for experimental evaluation purpose in the domain of Steganography. In the next section 3 an overview of the proposed and adopted Steganographic schemes in papers [Das17-Das16] have been put forth.

3. Overview of Proposed Steganographic Schemes [Das17-Das16]

This section outlines a detailed discussion of the proposed steganography algorithms i.e Simple LSB (SLSBS), Variable LSB (VLSBS) and MSB-LSB schemes undertaken in the research work from papers [Das17-Das16].For implementing steganographic schemes, the cover image is taken in any format (.jpeg, .png etc) and it is converted into bitmap (.bmp) format since that offers lossless uncompressed image version. The following section outlines the proposed steganography schemes briefly.

3.1. Simple Least Significant Bit Substitution (SLSBS) Scheme

The Simple Least Significant Bit Substitution (SLSBS) method is very familiar and one of the preliminary steganography schemes that performs replacement of the least significant bit of each cover image pixel with respect to the embedding message bit. The simple condition of replacement is, if the message bit is 1 and the corresponding LSB of the cover image pixel where the message bit is to be embedded is 0 or the message bit is 0 and corresponding LSB of the cover image pixel is 1 i.e. whenever contradiction happens then only substitution is performed. Else, the LSB of cover image pixel remains unaltered. So, each cover image pixel suffers from 50% probability of being flipped. This scheme is popular because **i)** it is very simple **ii)** offers lower computational complexity in comparison to conventional standardized cryptographic schemes and **iii)** its ability to transfer data securely.

3.2. Variable Least Significant Bit Substitution (VLSBS) Scheme

To incorporate randomness & variation, in the Variable Least Significant Bit Substitution (VLSBS) scheme, a hashing algorithm is used that randomly maps pixel values of cover image to different targeted hash mapped pixel values each time where the message/data bit gets embedded. Thus that offers better security against confidentiality attacks & replay attacks, if launched by intruders as compared to SLSBS scheme.

Using the SLSBS scheme the message bits were being embedded in the cover image pixels sequentially (from 55^{th} pixel onwards since first 54 pixels contain essential information about image header and cannot be modified). But in the VLSBS scheme a hash algorithm is used that randomly maps the cover image pixels to discrete values, unevenly where the actual embedding of message bits is furnished. This incorporates randomness while embedding data bits and thus offers better security against attacks as launched by intruders or adversaries.

3.3. Most Significant Bit-Least Significant Bit (MSB-LSB) Substitution Scheme

Single bit LSB substitution is a renowned algorithm and it can only substitute a single bit of data in each carrier pixel (in this case carrier is image); there is no scope of embedding more data bits inside the cover medium. So, this devised scheme employs an algorithm to use MSB and LSB positions of cover image pixel to substitute, which can embed maximum 2 data bits. Thus the advantage lies in the fact that the image quality is not sacrificed much and it is identical to simple LSB substitution algorithm (degree of substitution is 1), but maximum 2 message bits can be embedded here, whereas Simple LSB could embed only 1 message bit.

Fig.4 and Fig.5 below depicts a sample input cover image and corresponding stego obtained by applying the aforesaid schemes for both small and large sample image sizes.

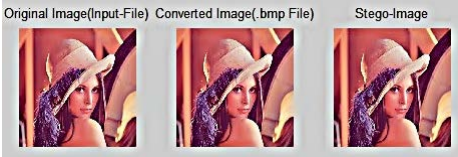

Fig.4 Original Image and Stego Image (for small cover image size)

Fig.5 Original Image and Stego Image (for large cover image size)

Thus, in this section, the various adopted schemes of Steganography as highlighted in the work [Das17-Das16] has been furnished in detail. The following section 4 discusses the experimental design overview and highlights some of the steganographic performance metrics undertaken for performance analysis of the aforementioned steganographic schemes.

4. Overview of Experimental Design and Performance Metrics

In this section a brief outline of the undertaken experimental design and performance metrics have been highlighted which have been employed to estimate the performance of the proposed steganographic schemes; VLSBS and MSB-LSB as depicted in papers [Das17-Das16].

4.1. Outline of Factors and Experimental Design

There are four primary factors which have been considered in experimental design for performance analysis purpose that includes **i)** the type of proposed steganographic approach (VLSBS and MSB_LSB schemes), **ii)** processor type (Intel Core i5 and Intel Pentium CPU N3530), **iii)** cover image size 462 KB (Lenna.png) and 1.27 MB (Peppers.jpg) and **iv)** data sizes (small having 3 characters and large having 14 characters) are also considered in some situations for analysis.

For the sake of experimental purpose, first both the algorithms (VLSBS and MSB-LSB) are simulated in MATLAB environment. Varying data inputs are given (all are character inputs: USA (3 characters: 24 bits), UNITED KINGDOM (14 characters: 112 bits) sizes. Following is the concise list of performance metrics that have been chosen for analysis purpose:

A 2^4 X 3 (2^k X r) factorial design = 48 experiments is considered taking into account the program execution time three times (replication r=3) adopting two different type of proposed steganographic approaches (VLSBS and MSB_LSB schemes), two different data sizes (small: 3 characters and large: 14 characters), two different processor types (Intel core i5 and Intel Pentium CPU N3530) and two different image sizes (Lenna: 462 KB and Peppers: 1.27 MB). The impact of the various factors is computed using the 2^4 X 3 factorial designs where each factors have two levels. Next the visual tests are conducted for further analysis purpose.

Additionally the Ranking method is undertaken to check the impact of all enlisted factors: image sizes, data sizes, type of processor, type of proposed steganographic approach at a glance.

Further corresponding to each proposed steganographic approaches (i.e SLSBS, VLSBS and MSB-LSB schemes) some popular metrics such as **(Mean Squared Error) MSE, (Peak Signal to Noise Ratio) PSNR, (Normalized Cross-Correlation) NCC, (Average Difference) AD, (Structural Content) SC, (Maximum Difference) MD and (Normalized Absolute Error) NAE, number of cover image pixels altered and required for embedding** are also computed to compare the performance among the proposed steganographic approaches as suggested from the literature survey metrics has been highlighted in section 2 of this paper.

In this section, the brief overview of factors and experimental design has been highlighted along with the enlisted performance steganographic metrics that have been analyzed. The following section details the performance computations and analysis done as per the aforesaid enlisted metrics.

4.2. Performance and Experimental Analysis

In this section the experimental data sets of 2^4 X 3 design and the computation analysis are discussed below:

The following Table.I enlists the undertaken factors and their corresponding levels.

Table.I. Factor Levels

Symbol	Factors	Level -1	Level +1
A	Type of proposed steganographic scheme (VLSBS and MSB-LSB)	VLSBS	MSB-LSB
B	Type of processor (Intel core i5 and Intel Pentium CPU N3530)	Intel core i5	Intel Pentium CPU N3530
C	Type of Cover Image Size (Small and Large)	Small: Lenna.png	Large: Peppers.jpg
D	Type of Data size (Small and Large) (in characters)	Small: 3 character ('USA')	Large: 14 characters ('UNITED KINGDOM')

The following Table.II depicts the factor level combinations and the mean program execution time as follows:

Here we have four main effects (A, B, C and D), six (AB, AD, BC, BD, AC, CD) two factor interactions, four (ABC, ABD, ACD, BCD) three factor interactions and one (ABCD) four factor interaction in this 2^4 X 3 design.

From the above highlighted design applying the Ranking method it can be concluded that best factor combination levels corresponding to minimum program execution time is when B=C=D= -1. It implies that on Intel core i5 processor with small cover image and data sizes, the program execution time is the least; thus the best.

After the computations it can be concluded that in decreasing order factors C, D, B, A, AC, CD interactions are important as compared to the other interactions (AB, AD, BC, BD, AD, ABC, ABD, ACD, BCD, ABCD that are negligible).

Thus it can be concluded that the **performance of steganographic schemes largely depends on the cover image size, data/message length size followed by the interaction between type of proposed steganographic scheme and the cover image size.** Next it can be inferred that the type of processor and adopted steganographic scheme has little effect on the performance of the steganographic algorithms.

Table.II. Factor Level Combinations

A	B	C	D	Program Execution Time (in sec) (Embedding + Retrieving Data) using the type of proposed steganographic scheme	Mean Program Execution Time (in sec)
-1	-1	-1	-1	(54.434, 51.975, 52.508)	54.434
1	-1	-1	-1	(54.68, 58.676, 56.818)	56.725
-1	1	-1	-1	(66.002, 68.522, 68.752)	66.002
1	-1	1	-1	(86.801, 89.213, 91.656)	87.26
1	1	-1	-1	(87.162, 88.357, 86.263)	88.99
1	-1	-1	1	(89.622, 90.872, 97.318)	92.604
-1	-1	-1	1	(96.477, 92.90, 96.302)	95.226
1	1	1	-1	(112.714,116.352,116.474)	115.18
-1	1	-1	1	(121.083, 120.709, 118.732)	121.083
1	1	-1	1	(130.432, 128.178,131.908)	130.172
-1	-1	1	-1	(131.542, 134.13, 137.807)	134.494
1	-1	1	1	(141.96,143.237, 142.767)	142.655
-1	1	1	-1	(178.376, 179.511, 176.556)	176.556
1	1	1	1	(179.451, 180.202, 178.542)	179.398
-1	-1	1	1	(230.408, 226.465, 234.575)	230.482
-1	1	1	1	(277.545,273.666, 276.702)	275.971

Thus it can be deduced that the **performance of steganographic schemes largely depends on the cover image size, data/message length size followed by the interaction between type of proposed steganographic scheme and the cover image size.** Next, it can be summarized that the type of processor and adopted steganographic scheme has little effect on the performance of the steganographic algorithms. The % variation unexplained and attributed to errors is 0.80% while the rest 99.2 % is explained by this regression model. Thus this model can be termed as a good model.
So, in the following Table.III only the important factor contributions are calculated ignoring the rest.

Table.III. Confidence Intervals and % Variation explained by the enlisted Factors

Factor	90 % Confidence Interval Effects		% Variation explained
C	38.196	41.384	43.6
D	28.902	32.09	25.6
AC	-21.891	-18.703	11.3
B	14.626	17.814	8.5
A	-17.924	-14.736	7.5
CD	7.286	10.474	2.7

Thus all the effects are significant since none of the above factors include 0 in its Confidence Intervals.

From the Quantile Quantile plot shown below in Fig.6, it can be concluded that the graph appears to be approximately linear and thus the data passes the normality test. Further the plot of residuals versus the predicted response as shown in Fig.7 clearly shows that the spread of residuals/errors is constant and the errors are randomly distributed.

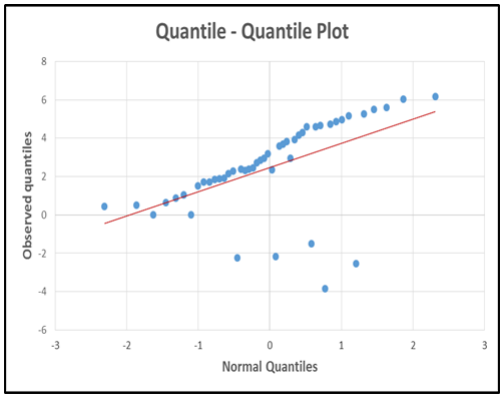

Fig.6. Quantile Quantile Plot

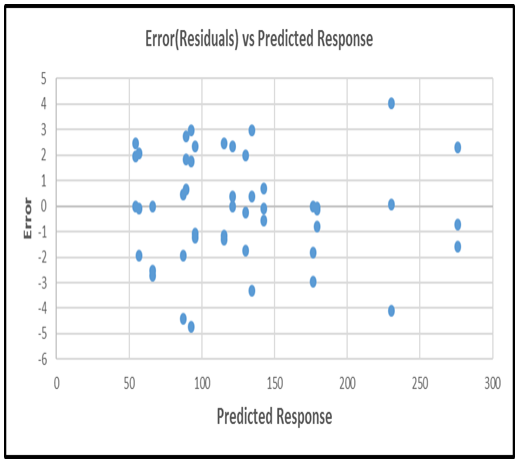

Fig.7 Scatter plot of Residuals versus Predicted Response

Thus in this section the experimental evaluations, designs, factor level combinations and outcomes have been discussed in detail. The next subsection highlights some of the adopted well known steganographic metrics which have been analyzed for the proposed steganographic schemes as highlighted in section 4 of this paper.

4.3. Comparison of Steganographic Metrics

As per the highlighted literature review conducted in the Steganography domain presented in section 2 of this paper, some of the well-known steganographic metrics (mathematical expressions of which are presented in Table IV below) have been computed here to compare the performance of proposed schemes SLSBS, VLSBS and MSB-LSB approaches for the purpose of further analysis. As a result, a varying data set to simulate the programs (Inputs: USA- 3 characters, INDIA - 5 characters, BOLIVIA -7 characters, AUSTRALIA - 9 characters and UNITED KINGDOM - 14 characters) have been considered and accordingly the following metrics have been computed that is enlisted in the Table.V and Table. VI below.

Further a comparative study of both the VLSBS and MSB-LSB schemes is facilitated here. The number of cover image pixels required for embedding data bits as well as the number of cover image pixels altered in MSB-LSB scheme is lower as compared to its VLSBS counterpart. **Thus MSB-LSB scheme performs better than VLSBS scheme.** The plots of relevant graphs have been shown in Fig.8 and Fig.9 below. Fig.10 shows the histogram of the original cover image and stego image that shows that there is not much alteration, hardly visible between original cover and stego image.

Table.IV. Mathematical Expressions of Image Steganographic Metrics

Mean Square Error	$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})$
Peak Signal to Noise Ratio	$PSNR = 10\log\frac{(2^n-1)^2}{MSE} = 10\log\frac{255^2}{MSE}$
Normalized Cross - Correlation	$NCC = 10\log\frac{(2^n-1)^2}{MSE} = 10\log\frac{255^2}{MSE}$
Average Difference	$AD = \frac{\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k}-x'_{j,k})}{MN}$
Structural Content	$SC = \frac{\sum_{j=1}^{M}\sum_{k=1}^{N}x_{j,k}^2}{\sum_{j=1}^{M}\sum_{k=1}^{N}x'^2_{j,k}}$
Maximum Difference	$MD = Max(\lvert x_{j,k} - x'_{j,k}\rvert)$
Normalized Absolute Error	$NAE = \frac{\sum_{j=1}^{M}\sum_{k=1}^{N}[O(x_{j,k})-O(x'_{j,k})]}{\sum_{j=1}^{M}\sum_{k=1}^{N}[O(x_{j,k})]^2}$

Table.V. Steganographic Metric Computations(Image Lenna)

LENNA							
USA							
	MSE	PNSR	NCC	AD	SC	MD	NAE
SLSB	0.000034332	92.7738	1	-0.0000038147	1	1	0.0000001845
VLSB	0.0000076294	99.3059	1	0.0000076294	1	1	0.000000061501
MSB- LSB	0.0000076294	99.3059	1	-0.000022231	1	1	0.0000001994
India							
SLSB	0.000034332	92.7738	1	-0.0000038147	1	1	0.00000027675
VLSB	0.000019073	95.3265	1	-0.000011444	1	1	0.00000015375
MSB- LSB	0.000015259	96.2956	1	0.0000076294	1	1	0.000000123
Bolivia							
SLSB	0.000038147	92.3162	1	-0.000022888	1	1	0.0000003075
VLSB	0.000038147	92.3162	1	-0.0000076294	1	1	0.0000003075
MSB- LSB	0.000019073	95.3265	1	-0.0000038147	1	1	0.00000015375
Australia							
SLSB	0.000034332	92.7738	1	-0.000026703	1	1	0.00000027675
VLSB	0.00005722	90.5553	1	-0.0000038147	1	1	0.00000046126
MSB- LSB	0.000019073	95.3265	1	-0.0000038147	1	1	0.00000015375
United Kingdom							
SLSB	0.000038147	92.3162	1	-0.0000076294	1	1	0.0000003075
VLSB	0.000045776	91.5244	1	-0.000015259	1	1	0.00000036901
MSB- LSB	0.000022888	94.5347	1	-0.000015259	1	1	0.0000001845

Table.VI. Steganographic Metric Computations(Image Pepper)

PEPPER							
USA							
	MSE	PNSR	NCC	AD	SC	MD	NAE
SLSB	0.00000089306	108.622	1	-0.000000099229	1	1	0.0000000079047
VLSB	0.00000099229	108.1644	1	-0.00000059537	1	1	0.000000008783
MSB- LSB	0.00000029769	113.3932	1	-0.000000099229	1	1	0.0000000026349
India							
SLSB	0.0000006946	109.7134	1	-0.000000099229	1	1	0.0000000061481
VLSB	0.0000011907	107.3726	1	-0.00000019846	1	1	0.000000001054
MSB- LSB	0.00000059537	110.3829	1	-0.00000039692	1	1	0.0000000052698
Bolivia							
SLSB	0.0000013892	106.7031	1	-0.00000039692	1	1	0.000000012296
VLSB	0.0000006946	109.7134	1	-0.00000029769	1	1	0.0000000061481
MSB- LSB	0.00000049615	111.1747	1	-0.00000049615	1	1	0.0000000043915
Australia							
SLSB	0.0000011907	107.3726	1	-0.0000011907	1	1	0.00000001054
VLSB	0.0000010915	107.7505	1	-0.0000006946	1	1	0.0000000096613
MSB- LSB	0.00000049615	111.1747	1	-0.00000029769	1	1	0.0000000043915
United Kingdom							
SLSB	0.0000016869	105.8599	1	-0.00000129	1	1	0.000000014931
VLSB	0.00000129	107.025	1	-0.000000099229	1	1	0.000000011418
MSB- LSB	0.0000006946	109.7134	1	-0.00000029769	1	1	0.0000000061481

From the Table. V and Table. VI, it is clear that the **Peak Signal to Noise Ratio (PNSR)** value range between 91.5244 dB to 113.3932dB (high value implies good performance). **Mean Squared Error (MSE)** value is very low for all experiments. The **Normalized Cross Correlation (NCC), Structural Content (SC)** is 1 for all experiment which implies that there is high similarity between cover image and generated stego image. **Average Difference (AD)** between two selected pixel values of cover and stego image is very low. **Maximum Difference**

(MD) is used to measure the cover and stego and the compressed quality of stego image, whose value is low means high quality result. **Normalized Absolute Error (NAE)** is the statistical difference between the cover and stego image. The small value indicates high quality.

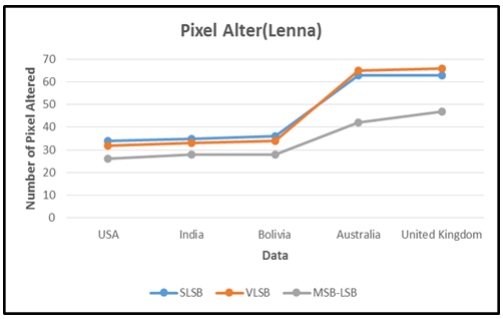

Fig.8 Number of pixels altered in Small Image size (Lenna.png: 462 KB)

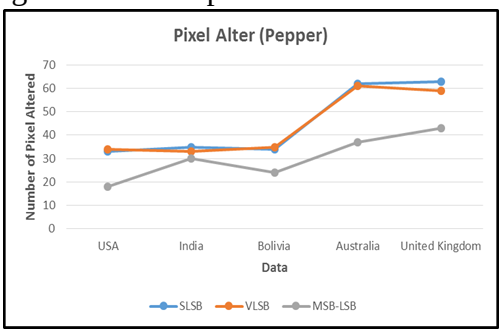

Fig.9 Number of pixels altered in Large Image size (Peppers.jpg: 1.2 MB)

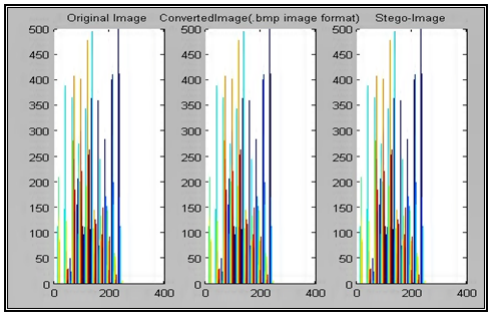

Fig.10. Histogram of Original and Stego Image

Thus in this section the experimental evaluations, designs, factor level combinations and outcomes have been discussed in detail. Besides some of the adopted well known steganographic metrics have been analyzed for the proposed steganographic schemes as highlighted in the former section 3 of this paper. Results reveal that the MSB-LSB scheme performs better as compared to its VLSBS or SLSBS counterparts in most cases. The following section puts forth the conclusion.

5.Conclusion

In this paper, performance analysis is done to compare performances of two modified LSB Steganography algorithms namely: VLSBS and MSB-LSB which have been put forth as a security model in papers [Das17-Das16]. An extensive literature survey has been conducted in

the Steganographic domain, so as to get the idea of well-known steganographic metrics that are widely employed nowadays to compare the performances of aforementioned steganographic schemes. The primary factors that affect the performance of steganographic algorithms have been enlisted. Further a 2^4X 3 experimental design (48 experiments) is undertaken to quantify the effects of the enlisted factors.

After computation it has been observed that the program execution time of steganographic schemes largely depends upon the cover image size, data/message length size followed by the interaction between type of proposed steganographic scheme and the cover image size. Also from the computations of various steganographic metrics like (Mean Squared Error) MSE, (Peak Signal to Noise Ratio) PSNR, (Normalized Cross-Correlation) NCC, (Average Difference) AD, (Structural Content) SC, (Maximum Difference) MD and (Normalized Absolute Error) NAE, number of cover image pixels altered and required for embedding it can be concluded that the performance of proposed MSB-LSB scheme is better as compared to its VLSBS or SLSBS counterpart.

References

[Bed16]. Punam Bedi, Veenu Bhasin and Tarun Yadav, "2L-DWTS - Steganography technique based on second level DWT" , 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 21-24 Sept., 2016, pp:1533-1538, ISBN: 978-1-5090-2029-4. http://ieeexplore.ieee.org/document/7732266/

[Bou16]. Dalila Boughaci, Abdelhafid Kemouche and Hocine Lachibi, "Stochastic Local Search Combined with LSB Technique for Image Steganography", 2016 13th Learning and Technology Conference (L&T), 10-11 April , 2016, pp:36-44, ISBN: 978-1-5090-3394-2.http://ieeexplore.ieee.org/document/7562863/

[Das17]. Ria Das and Punyasha Chatterjee "Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography" in International Conference on High Performance Compilation, Computing & Communications (HP3C-2017) in Kuala Lumpur, Malaysia, March 22-24, 2017, published in ACM Digital Library,pp:17-22,ISBN: 978-1-4503-4868.https://dl.acm.org/citation.cfm?id=3069605

[Das16]. Ria Das and Indrajit Das, "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques" in 2nd IEEE International Conference on Research in Computational Intelligence and Communication Networks(ICRCICN), India, Sept. 23-25, 2016, Published in IEEE Xplore Digital Library, pp:296 -301,978-1-5090-1047-9. http://ieeexplore.ieee.org/document/7813674/

[Idb14]. Tarik Faraj Idbeaa, Salina Abdul Samad and Hafizah Husain, "Comparative Analysis of Steganographic Algorithms Within Compressed Video Domain", 2014 8th International Conference on Signal Processing and Communication Systems (ICSPCS), 15-17 Dec, 2014, ISBN: 978-1-4799-5255-7.http://ieeexplore.ieee.org/document/7021067/

[Jai15]. Mamta Jain and Saroj Kumar Lenka, "Secret Data Transmission using Vital Image

Steganography over Transposition Cipher" , 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 8-10 Oct. , 2015, pp:1026- 1029, ISBN: 978-1-4673-7910-6. http://ieeexplore.ieee.org/document/7380614/

[Jam14]. N.D. Jambhekar, C.A. Dhawale and R. Hegadi, "Performance Analysis of Digital Image Steganographic Algorithm", ICTCS '14, Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 14 - 16 Nov, 2014, ISBN: 978-1-4503-3216-3.https://dl.acm.org/citation.cfm?id=2677937&CFID=991879869&CFTOKEN=15691904

[Jer15]. S. Edward Jero, Palaniappan Ramu and S. Ramakrishnan, "Steganography in Arrhythmic Electrocardiogram Signal", 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), 25-29 Aug, 2015, pp: 1409- 1412, ISBN: 978-1-4244-9271-8.http://ieeexplore.ieee.org/document/7318633/

[Pra16]. Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain and K. Raja Sekhar, "Performance Evaluation Parameters of Image Steganography Techniques", 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), 6-7 May, 2016, pp:1-8, ISBN: 978-1-5090-1111-7.http://ieeexplore.ieee.org/document/7764399/

[Red16]. V. Praneeth Kumar Reddy and Annis Fathima A, "A Cost Effective Approach for Securing Medical X-ray Images using Chebyshev Map", 2016 International Conference on Recent Trends in Information Technology (ICRTIT), 8-9 April ,2016, ISBN : 978-1-4673-9802-2.http://ieeexplore.ieee.org/document/7569576/

[Ren14]. Yang Ren-er, Zheng Zhiwei, Tao Shun and Ding Shilei, "Image Steganography Combined with DES Encryption Preprocessing", 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, 10-11 Jan, 2014, pp: 323-326, ISBN:978-1-4799-3435-5. http://ieeexplore.ieee.org/document/6802697/

[Sin16]. Anuradha Singhal and Punam Bedi, "Local Binary Pattern Operator based Steganography in Wavelet Domain" , 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 21-24 Sept., 2016, pp: 826- 831, ISBN: 978-1-5090-2029-4.http://ieeexplore.ieee.org/document/7732148/

[Sir15]. B. Lakshmi Sirisha, S. Srinivas Kumar and B. Chandra Mohan, "Steganography based in-formation security with high embedding capacity", 2015 National Conference on Recent Advances in Electronics & Computer Engineering (RAECE), 13-15 Feb. , 2015, pp: 17- 21, ISBN: 978-1-5090-2146-8. http://ieeexplore.ieee.org/document/7510218/

[Sub13]. Mansi S. Subhedar and Vijay H. Mankar, "Performance Evaluation of Image Steganography based on Cover Selection and Contourlet Transform", 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 15-16 Nov. , 2013, pp: 172-177, ISBN:978-1-4799-2235-2. http://ieeexplore.ieee.org/document/6701498/

[Val16]. G. Vallathan, G. Gayathri Devi and A. Vinoth Kannan, "Enhanced Data Concealing

Tech-nique to Secure Medical Image in Telemedicine Applications", 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 23-25 March, 2016, pp: 186-190, ISBN: 978-1-4673-9338-6.http://ieeexplore.ieee.org/document/7566117/

[Waz15]. Raniyah Wazirali, Shaher Slehat and Zenon Chaczko, Grzegorz Borowik and Lucia Carrion, "Objective Quality Metrics in Correlation with Subjective Quality Metrics for Steganography", 2015 Asia-Pacific Conference on Computer Aided System Engineering (APCASE), 14-16 July, 2015, pp: 238- 245,ISBN: 978-1-4799-7588-4. http://ieeexplore.ieee.org/document/7287026/

Acronyms

[1] AD: Average Difference
[2] BER: Bit Error Rate
[3] CR: Compression Ratio
[4] DCT : Discrete Cosine Transformation
[5] DES : Data Encryption Standard
[6] DFT : Discrete Fourier Transformation
[7] DWT: Discrete Wavelet Transformation
[8] EPVD: Enhanced version of Pixel Value Difference
[9] IoT : Internet of Things
[10] IF: Image Infidelity
[11] IWT: Integer Wavelet Transformation
[12] LBG : Linde Buzo Gray
[13] MD : Maximum Difference
[14] MD5: Message Digest 5
[15] MSB-LSB : Most Significant Bit- Least Significant Bit
[16] MSE : Mean Squared Error
[17] NAE: Normalized Absolute Error
[18] NCC : Normalized Cross Correlation
[19] PRD: Percentage Residual Difference
[20] PSNR : Peak Signal to Noise Ratio
[21] SC: Structural Content
[22] SSIM: Structural Similarity Index
[23] SLS: Stochastic Local Search
[24] VLSBS : Variable Least Significant Bit Substitution
