Journal of Information and Technology

Information Security through Improved Image Steganography Algorithm

Elsie Wangui Ngatia & Dr. Alice Njuguna

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information and Technology
Volume 1||Issue 1||Page 28- 45||January||2018|
Email: stratfordjournals.org

Information Security through an Improved Image Steganography Algorithm

[1*] Elsie Wangui Ngatia and [2]Dr. Alice Njuguna

[1*]Postgraduate Student, KCA University

[2]Lecturer, KCA University

***E-mail of corresponding author: elsywangu@gmail.com**

***How to cite this article*: Ngatia E., W. & Njuguna A. (2018), Information Security through an Improved Image Steganography Algorithm, *Journal of Information and Technology* Vol 1(1) pp. 28-45.**

Abstract

Steganography is the data hiding technique which allows hiding secret message or image within a larger image or message such that the hidden message or an image is undetectable. It is a very useful method for secret information transmission. This research proposed security of information through an image hiding steganographic method, of hiding an image within a cover image. This steganographic method aims to minimize the visually obvious and numerical differences between the cover image and a stego image with increase in the size of the payload. The proposed improved algorithm uses the binary codes which is the binary representation of pixels inside the image. This algorithm make use of improved least significant bit (LSB) technique, which is a popular technique in steganography ,in which least significant bits of cover are altered by secret data bits. The proposed method integrates randomization algorithm which improve the security of LSB scheme. The bits of the secret image are embedded in random pixels of the cover image. The method enhances the security of the LSB technique by randomly dispersing the bits of secret image in the cover image which makes it harder for unauthorized people to extract the original image. Since all the secret image bits are embedded in the cover image the exact secret image can be regenerated from the stego-image and thereby the image quality is preserved by the system. The research implements steganography for images, with an improvement in both security and image quality.

Keywords: *Information security, Image, Steganography and Algorithm*

1.0 Introduction

1.1 Background of the Study

Steganography is defined as the art of hiding information within any media file in ways that prevent the disclosure of the hidden information to unauthorized recipients (Katzenbeisser & Petitcolas 2010; Zoran , Michael & Sushil, 2010) Thus, it can be used as an information security approach

to secure stored data or data exchanged over non secured communication channels(Atallah & Al-Shatnawi 2012). Steganography carries the information secretly by concealing the very existence of information in some other media files such as image, audio, video, or text files. The information to be concealed is called the secret message or simply the secret; the content used to embed information is called the cover media, and the cover along with the secret is called the stego media (Rajkumar, Ravi & Kamaldeep, 2011).

As the development of internet technologies increases, the transmission of digital media is now-a-days convenient over the networks. But secret information broadcasting over the network suffers from severe security overhead. So, self-protective of secret information for the period of transmission becomes an important matter (Prabakaran, Bhavani & Rajeswari, 2013). Though cryptography changes the message so that it cannot be understood but this can generates curiosity level of a hacker. It would be rather more practical if the secret message is smartly embedded in another media so that no one can guess if anything is hidden there or not (Akhtar, Johri, Khan, 2013). This idea results in steganography, which is a branch of information hiding by camouflaging secret information within other information.

In any communication, security is the most important feature. With the advancement of technology and the wide use of World Wide Web for communication increase the challenges of security (Atallah & Al-Shatnawi 2012). However, the challenges can be controllable with the advanced technologies of secure networks but every time these technologies may not be reliable for communication of secret information over a long distance that produce a need of additional security mechanisms to secure secret information. According to Natasha, (2015), to provide the security two techniques has been used widely, Cryptography and Steganography. Cryptography is used to scramble the information, deals with changing the meaning and appearance of message. It changes the plain text into cipher text by the process of encryption, uses the mathematical techniques and various algorithms such as public key cryptography, private key or symmetric and asymmetric algorithm for securing the information while steganography hides the data from third parties (Rengarajan, *et al.*, 2012). However, cyber attacker can easily arouse the text and intercepts the communication between two separate users to modify, inject, or drop any communication packet. To reduce the limitations posed by the hackers a two tier architecture method can be used which applies both cryptography and steganography (Natasha, 2015).

1.2 Statement of the Problem

Numerous cases of hacking into individual e-mail accounts and organization servers have been growing steadily as more people embrace online lifestyle. As Feldman (2012) observe that data computing is rife with history of leaks, both accidental and deliberate that has led to the recognition of the privacy risks of data deployment. The author goes on to cite the flaws in Google docs and spreadsheets that allowed customer's documents to be viewed by unauthorized users that was attributed to bugs or design errors within cloud's provider's software. In addition, the author cites cases where popular photo hosting sites such as Facebook and Flickr have suffered from flaws that have leaked user's private pictures.

With fast growing network, many people utilize the various applications to transfer digital image data. Most people share their personal images with other users using social applications. Hacking attacks on these applications can cause great losses to the user security which can lower the number of active users and using the services online. (Grgic, 2001). To prevent the hacking attacks on the

various architectures, there is various data security mechanisms for image, video or text data, (Karam, 2008).

Subsequently, use of ICT has enabled organizations to operate their businesses much faster and more conveniently (El-Hoby, 2014). While this has been done there are some problems still faced by individuals, organizations such as lack of proper security mechanisms by using only one method of hiding data like cryptography. Cryptography alone has proved not to be sufficient enough in proving security. Therefore this study was conducted so as to establish information security through an improved image steganography algorithm.

1.3 Specific Objectives

i. To design the improved least significant bit (LSB) algorithm.
ii. To develop and test an improved least significant bit (LSB) steganography method.
iii. To simulate the improved least significant bit (LSB) method versus mean square error (MSE) and peak signal to noise ratio (PSNR) parameters.

1.4 Research Questions

i. How is improved LSB algorithm defined and designed?
ii. How is improved LSB steganography method developed and tested?
iii. How does improved LSB method versus MSE and PSNR parameters simulated?

2.0 Literature Review

2.1 Theoretical Model

The literature reviews and analyzes several themes related to information security using image steganography while transmitting information.

2.1.1 An Information-Theoretic Model for Steganography

Most existing formal models for information hiding have not addressed steganography but the more general problem of hiding information with active adversaries in watermarking and fingerprinting applications. This is different from steganography because the existence of a hidden message is known publicly. Since most objects to be protected by watermarking and fingerprinting consist of audio, image, or video data, these areas have received the most attention so far. A large number of hiding techniques and domain-specific models have been developed for robust, imperceptible information hiding (Cox, Miller, & loom, 2002). Ettinger (2002) models active adversaries with game-theoretic techniques. We are aware of only two related information-theoretic models for steganography.

Mittelholzer (1999) defines steganography (with a passive adversary) and watermarking (with an active adversary) using an information-theoretic model. A stego system is required to provide perfect secrecy for the embedded message in sense of Shannon, and an encoder constraint is imposed in terms of a distortion measure between cover text and stego text. The expected mean squared error is proposed as a possible distortion measure. The adversary's task of distinguishing between an innocent cover message *C* and a modified message *S* containing hidden information is interpreted as a hypothesis testing problem. The security of a steganographic system is quantified in terms of the relative entropy (or discrimination) between the distributions of *C* and *S*, which yields bounds on the detection capability of any adversary. It is shown that secure steganographic schemes exist in this model provided the cover text distribution satisfies certain conditions. A

universal stego system is presented in this model that needs no knowledge of the cover text distribution, except that it is generated from independently repeated experiments.

2.1.2 Multi- level Encryption Algorithm model

According to Khan and Tuteja (2015) security goals of data include three points namely: availability, confidentiality and integrity. This, therefore, means that in addressing security issues in data communication, the three points are important in guaranteeing data security. Khan and Tuteja (2015) propose a system which uses multilevel encryption and decryption to provide more security for data storage. It thus, implies that, an algorithm that can address the three concerns is what is missing in the current architecture and algorithm implementation. Khan and Tuteja (2015) observe that, multilevel encryption and decryption can secure communication over distributed and connected resources. In their proposed system Data Encryption Standard (DES) and RSA algorithm is used to generate encryption when user uploads text files and inverse DES and RSA algorithm to generate decryption when user download file from the storage. This is because single level encryption may be cracked by hackers. Thus, the key issue is therefore, to provide a multilevel encryption control in order to harden the system for attackers.

Nigoti (2013) observes that in existing systems only single level encryption and decryption is applied to the data storage. The authors, therefore, point that the continued use of single level encryption and decryption of data in the will continue to cause concern among users. The proposed two tier encryption promises to reduce data being accessed by an unauthorized user. As Khan and Tuteja (2015) observe that even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is very difficult task without a valid key. This, therefore, according to the authors will provide more security for data transmission and storage than using single level encryption. The drawback of the proposed system is that it may be time consuming in terms of computation. The use of DES and RSA in encryption and decryption creates complexity which in itself is a drawback.

2.2. Empirical Review

According to (Arora, 2015), hybrid image security approach has been used. The techniques included in the combination are image compression, cryptography and steganography. The compression was used to reduce the size of the image and blowfish for encryption purposes. Blowfish offers maximum throughput and energy efficiency.

According to Attri (2015), the author presented the dual layer of security for data, in which first layer is to encode data using Least Significant Bit (LSB) image steganography method and in the second layer encryption of the data using Advance Encryption Standard Algorithm (AES). Steganography does not replace the encryption of data but provides extra security. The secret text message is hidden behind the digital image file and the image file is then encrypted using AES encryption algorithm.

According to Pattewar, (2014), the author introduced a new way for originating the existing concept that is separable reversible data hiding mainly, the concept of separable reversible data hiding technique was bases on steganography. Text was used as a hidden data. Then the cover media is encrypted and hide the data to get the data as well as cover media as per the provision. This method is cumbersome because there are three procedures which are used.

According to Preet, (2014), the author proposed a method which combined three security techniques that is steganography, cryptography and watermarking. The method does not only hide

the information but produce better results for MSE. It also shows that PSNR and embedding capacity is not there after the noise attack. Various parameters like PSNR, MSE and embedding capacity proved better results than the traditional approach.

According to Meyyappan, (2012), a method was proposed which include the combination of encryption and steganography by using the DES algorithm and LSB method. DES is used to encrypt secret message and LSB method is used to hide encrypted secret image into cover image. To produce better imperceptibility levels this proposed method provides a higher similarity between cover and stego images as a result. The eavesdroppers can hardly see the information with their naked eyes when the two techniques are combined. The proposed techniques is effective for secret data communication

According to Rashedul, (2014), the author developed a new technique to hide large data in Bitmap image using filtering based algorithm. This method uses the concept of status checking for the purpose of insertion and retrieval of message. The proposed method is very efficient to hide the secret information inside an image.

According to GundaSai Charnl, (2015) the author proposed a highly secured chaos based image steganography method. Encryption has been added to steganography technique at two levels because of Caesar cipher and chaos encryption technique. The proposed method uses cover in the spatial domain for hiding the secret information. This proposed method has added security and better performance when compared to the traditional LSB technique.

According to Ashiwini, (2014), the author provided DCT which is used for lossy compression and for encryption of secret data block ciphers are used. Although these approaches are relatively secure, high processing time is required, it involves computational overheads and processing speed is less. A hybrid approach is required for compression, double encryption and steganography. To increase encryption speed, reduce processing time and also provides more security, authentication, authorization, integration of data and also maintains confidentiality.

According to Soni, (2012), the author proposed a method for embedding data in images where the data is first encrypted and then embedded within an image with the help of steganography algorithm. The method is efficient when applied to those mages whose pixels are scattered. The image is then partitioned into four block levels and then the data will be embedded into selected the four sub blocks values depending upon the key. The algorithm needs few steps and it can embed data more efficiently. The quality of stego image is greatly improved when this method is used.

Table 1: Summary of Literature Review

Author	Method	Drawback	Advantages
Arora, (2015)	Hybrid image security approach	Low PSNR value and secret key is as big as the message	Good quality stego image Embeds the message very fast
Attri (2015)	Dual layer suing SLB and AES	Tampered data is not always recoverable	Highly secure
Pattewar, (2014)	Reversible data hiding technique	Very complex computations, time consuming	Highly secure, Good stego image quality
Preet,(2014)	Uses cryptography, steganography and watermarking	PSNR value is average	Highly secure, less embedding time
Meyyappan, (2012)	Uses encryption and steganography by using DES an LSB	Easily vulnerable to attacks	Highly secure, simple and easy to implement
Rashedul, (2014)	Hides data in bitmap image	Third party will be able to detect the message	Good image quality, improved security
GundaSai (2015)	Uses chaos based image adaptive method	Time taken to detect edges and storage space increases with increase in the number of pixels	Less embedding time, reduces attacks
(Ashiwini (2014)	Uses DCT for lossy compression	High processing time is required	Highly secure
Soni, (2012)	Embeds data in an image	Vulnerable to brute force attacks	Simple and easy to implement

2.3 Steganography

Is a way of hiding information to conceal the existence of a message? Original message is hidden within a carrier such that the changes that occur in the carrier are not observable (Kumar, 2010).

There are various steganography techniques which are used to cover the message. They include;

2.3.1 Image Steganography

According to Bailey, (2012) image steganography involves taking the cover object as image in steganography is known as image steganography. In this method pixel intensities are used to hide the information. Also involves concealing data inside picture which can be undoubtedly be spread over the World Wide Web.

Image Steganography Model

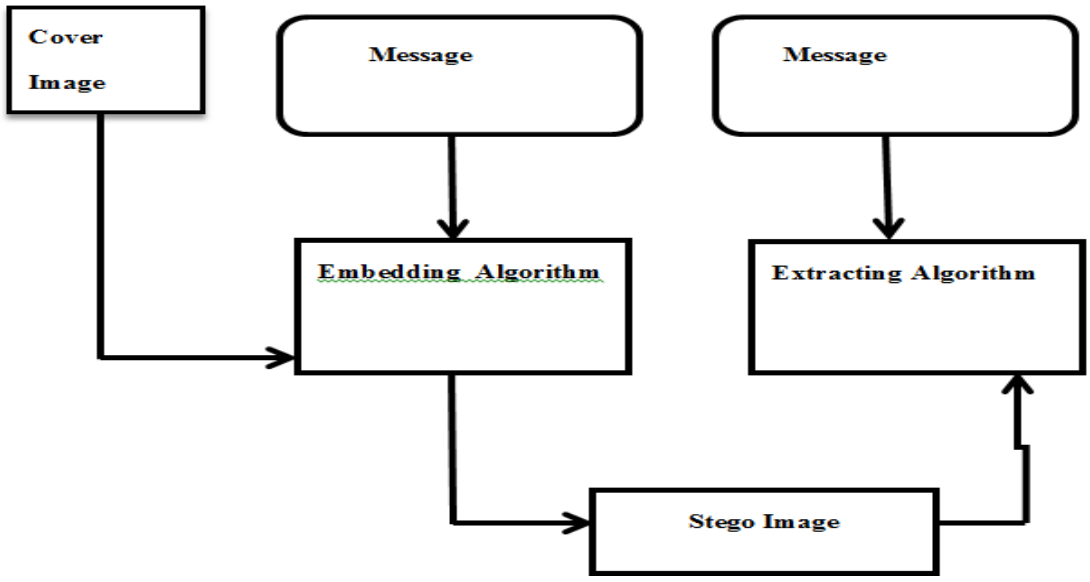

Figure 1: Image Steganography Model

The research used image steganography because images are the most popular cover objects used for steganography. In the domain of digital images many different mage file formats exist, most of them for specific applications. For different image file formats, different steganographic exist (Morkel, 2005).

Table 2: Comparisons of Different Steganographic Techniques

Technique	Security	Capacity	Transparency	Integrity	Temper resistance	Robustness
Text steganography	High	Low	Low	Low	High	Low
Image steganography	High	High	Low	High	High	High
Audio steganography	Low	Low	Low	Low	High	Low
Video steganography	High	High	High	Low	High	Low

(Kumar , 2015)

Some of the algorithms used in image Steganography include: least significant bit, Jsteg and F5 algorithms.

3.0 Research Methodology

The study took the design of both descriptive research (what is going on) as well as explanatory research (why it is going on) perspectives. These two designs were reinforced by use of System Development methodology. According to Nunamaker,(1991), the principle parts of a system development life cycles are; Construct a conceptual framework, Develop a system architecture, Analyze and design the system, Build the system and Experiment, and observe and evaluate the system.

4.0 Conceptual Modelling and Field Studies

4.1. Conceptual Model

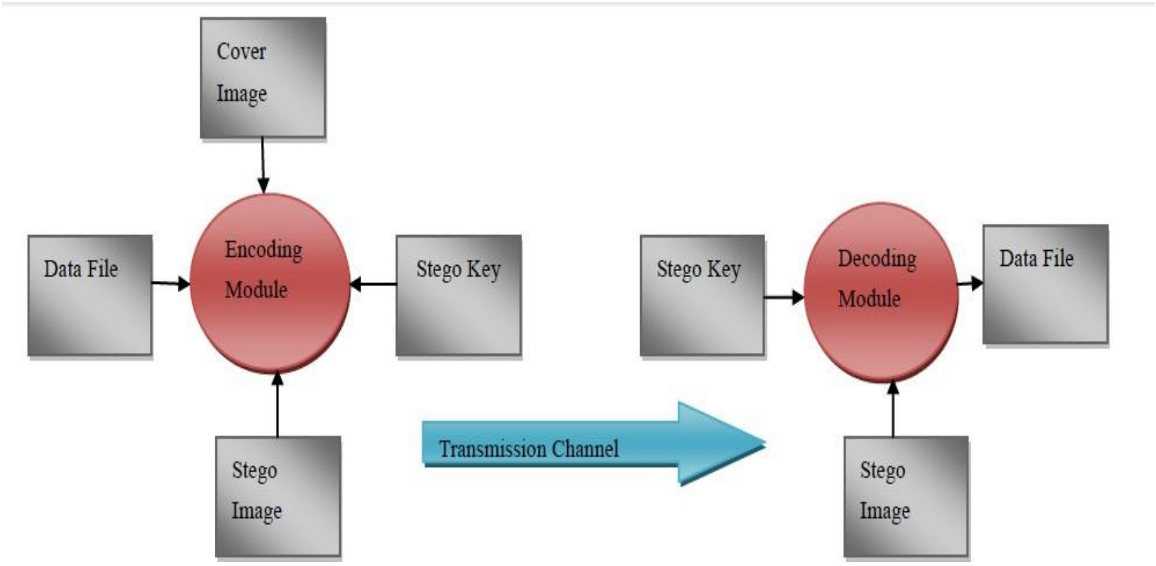

Figure 2. Conceptual Model

4.2. Design

The image steganographic technique in this project can be explained using this simple block diagram.

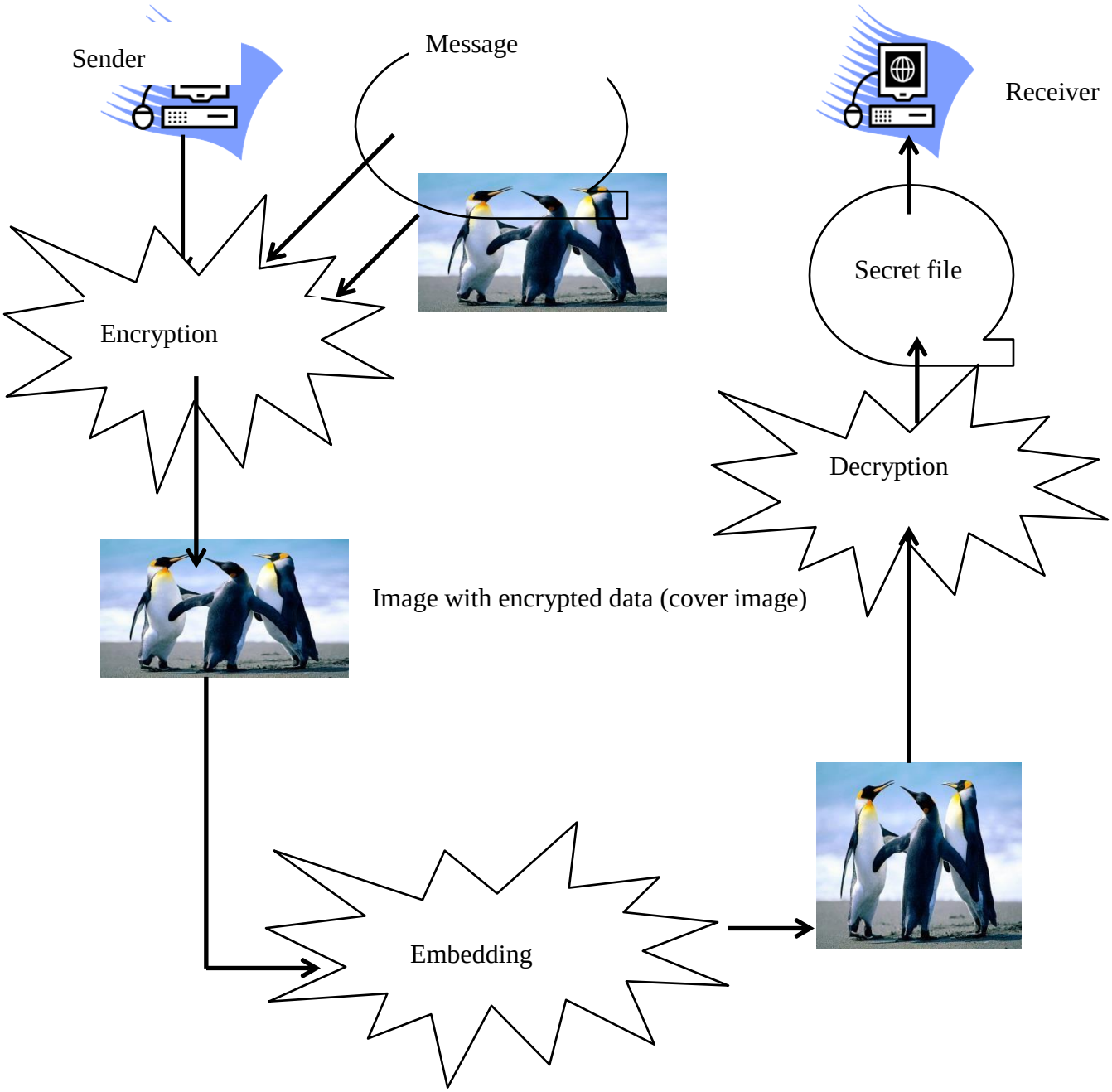

Figure 3: Steganographic Model

The procedure for data hiding using steganographic application in this research is as follows

- The sender encrypt the data using blowfish algorithm
- The sender then uses improved LSB algorithm to embed data in an image.
- The carrier file acts as an input for the decryption phase

- The image in which data is hidden is sent to the receiver using a transmission medium e.g. web or email.
- The receiver receives the carrier file and places the image in the decryption phase
- In the decryption phase, the original text document is revealed.
- The decryption phase decrypts the original text document using improved LSB decoding and decrypts the original message.

As explained in the block diagram above, the data hiding and data extracting was done in three phases. These include: Encryption Phase, Decryption Phase Embedding Phase and Simulation Phase.

4.3 Constructing Data Flow Diagram

The data flow diagrams can be constructed by dividend the process into levels such as DFD0, DFD1 for constructing the data flow diagram. In this process the following steps are followed.

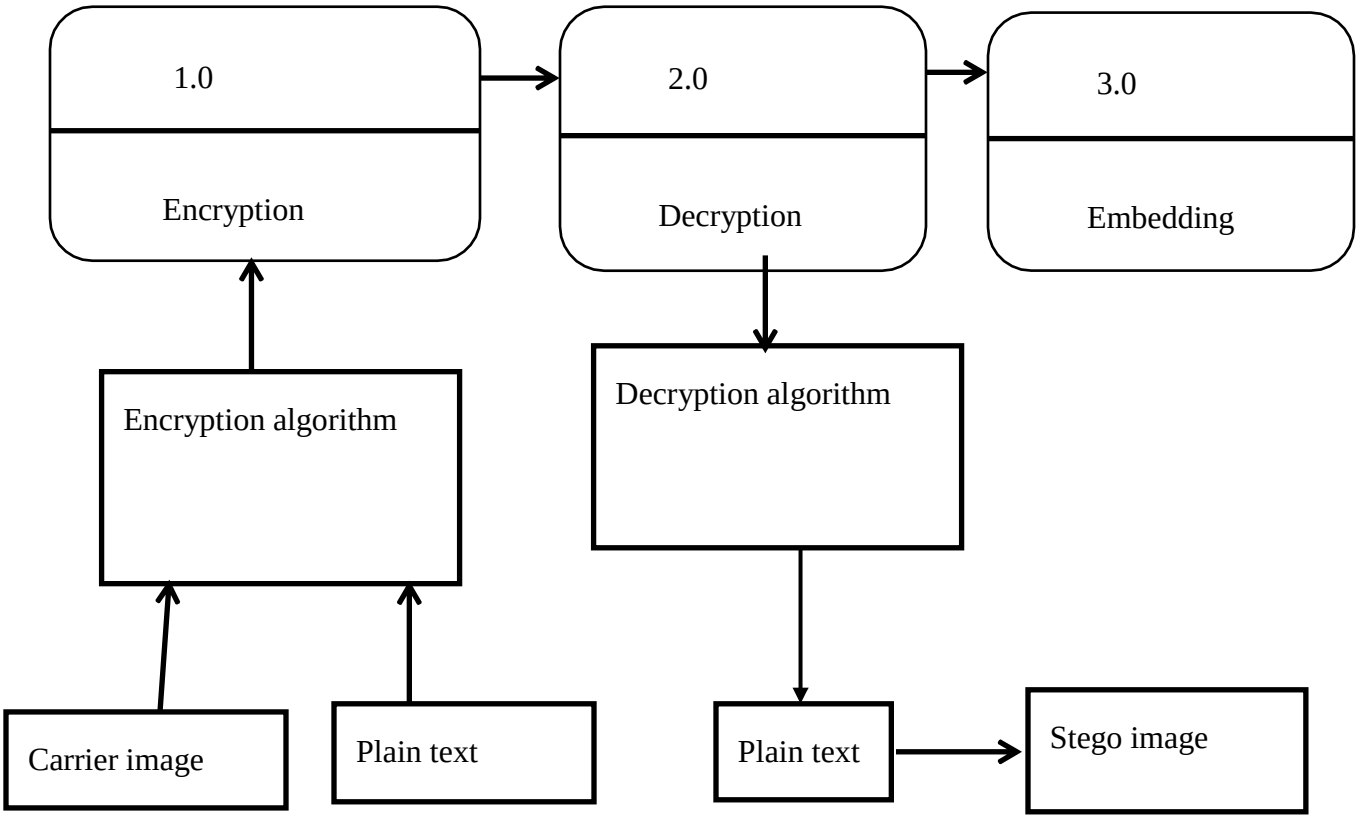

Figure 4: Data Flow Diagram Level 2

In this data flow diagram, the secret data is sent into the encryption phase for embedding the data into an image for generating the carrier image. The next part is which the carrier image is forwarded to decryption phase. Then the decryption phase is where the data is extracted from the image and displays the original message.

4.4. Activity Diagram

The message is sent by the sender to the receiver. The sender sends text as well as image to the encryption phase. The encryption phase uses the blowfish encryption algorithm by which the carrier image is generated. The encryption phase generates the carrier image as output.

The activity diagram below explains the procedure used in this research project.

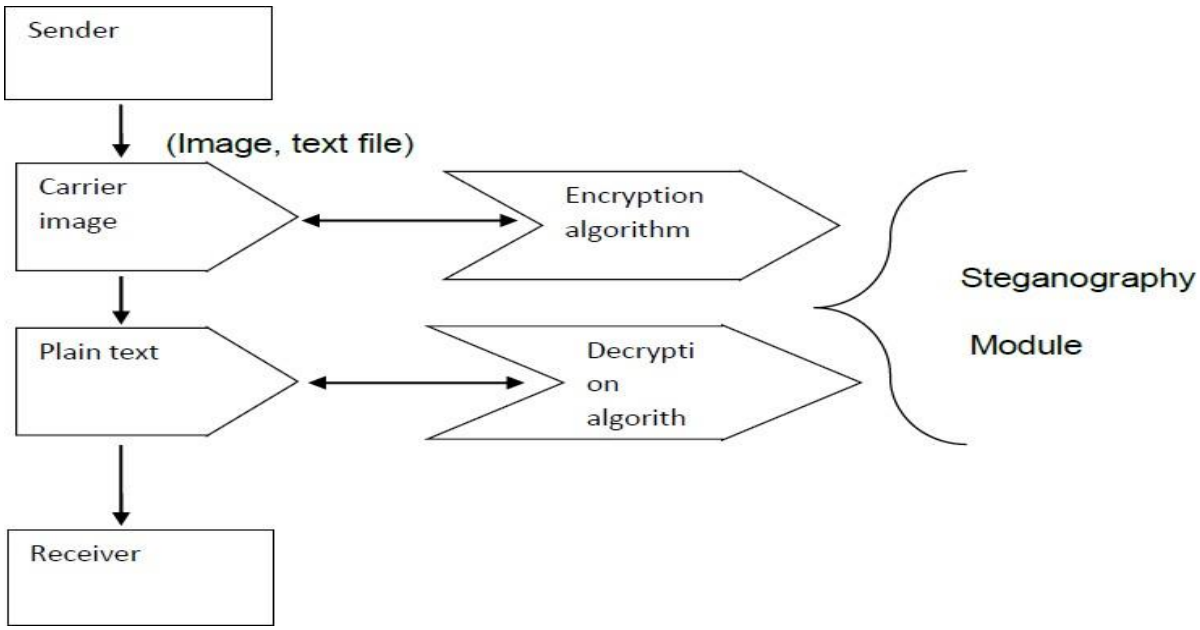

Figure 5: Activity Diagram

The carrier image is given as input to the next phase which is decryption phase. The decryption phase uses the blowfish algorithm for decrypting the original text from the image so that the decryption phases generate the plain text.

5.0 Implementation and Testing

5.1. Implementation Model

Encryption/Decryption Layer

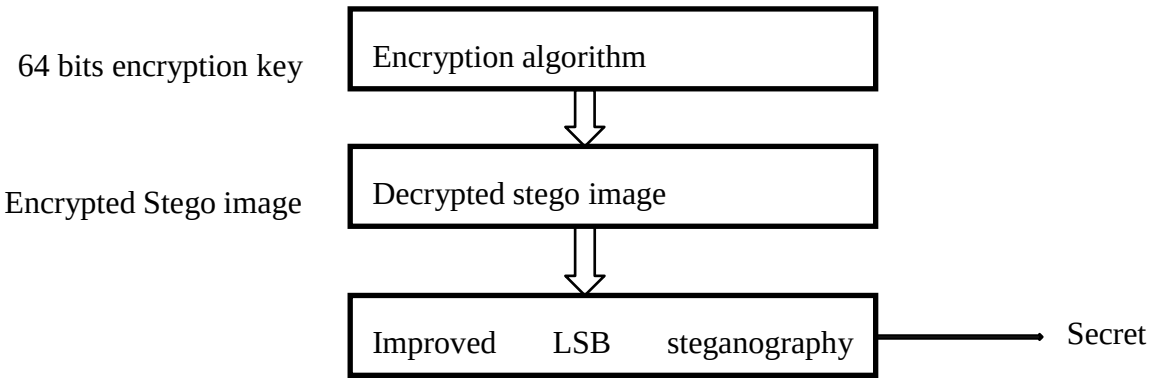

Figure 6: Encryption/Decryption layer

Steganography layer

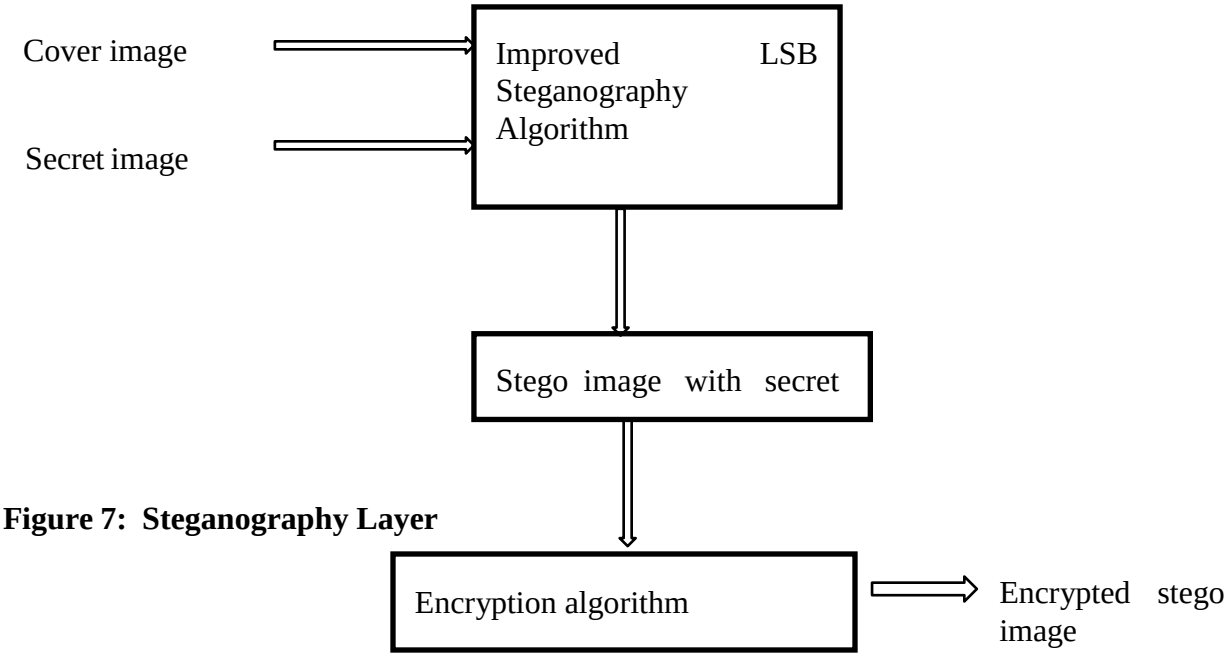

Figure 7: Steganography Layer

5.2. Method Implementation

The proposed method was implemented in Java programming language. The choice of language in this case was not unusual. The important value proposition of this platform according to Sun is its ability to "Write once, run anywhere" This means that the most important promise of Java technology is that you only have to write your application once for the java platform and then you will be able to run it everywhere. Java support is becoming ubiquitous. It is integrated in all major operating systems. Its built into the popular web browsers. Other benefits of java platform include the following;

i. Java is very secure and it runs huge enterprise applications both web and desktop such as twitter therefore its security reliability is proven.
ii. Java is fast and hence the encryption, hiding, decryption and extraction of the data will take a significantly less time and it won't affect other operations.
iii. Java can run on both web, desktop and mobile applications hence the method can be integrated into all these platforms.

The method is implemented in three phases.

5.2.1. Encryption Module

In this module, the sender sends the data as well as the image file which acts as carrier image to transfer the data to destination. In this research work I have used bitmap images as carrier image because bitmap images are highly resistant compared to jpeg images. In this phase the text

message will be embedded into the image file. The embedding will be done using the improved least significant bit algorithm. The least significant bit algorithm selects randomly the least significant bits of each pixel and replace the significant bits of the text message such that the message will be encrypted into the image.

Figure 8: Screen Shot of Encryption Phase

In the encryption phase, the sender gives the carrier file as the text message to be transferred to the destination. In this research project, I have taken a bit map image as a carrier file. The entered message is encrypted by using a secret key that is also used for decryption.

5.2.2. Decryption Module

In this module the receiver receives the carrier image from the sender. The receiver then sends the carrier image to the decryption phase. In the decryption phase, the same improved least significant bits is implemented for decrypting the least significant bits from the image and merger in an order to frame the original message bits. If the message is decrypted successfully, the file is decrypted from the carrier file and accessed as an original text document.

5.2.3. Embedding Module

In this module the Message is embedded in an improved LSB algorithm where bits are selected randomly thus making hacking of information hard because the attacker cannot understand which bit has been used to hide the information in an image.

5.2.4. Simulation Module

In this module two parameters are used for measuring the hiding capacity and image quality of the data. MSE and PSNR are used to measure.

5.2.5. Encryption using Improved Least Significant Bit

The encrypted message is hidden in the last four bits of the selected image. The bits where the message is hidden is chose randomly and it also embedded into the message so that it will be determined when decoding the message.

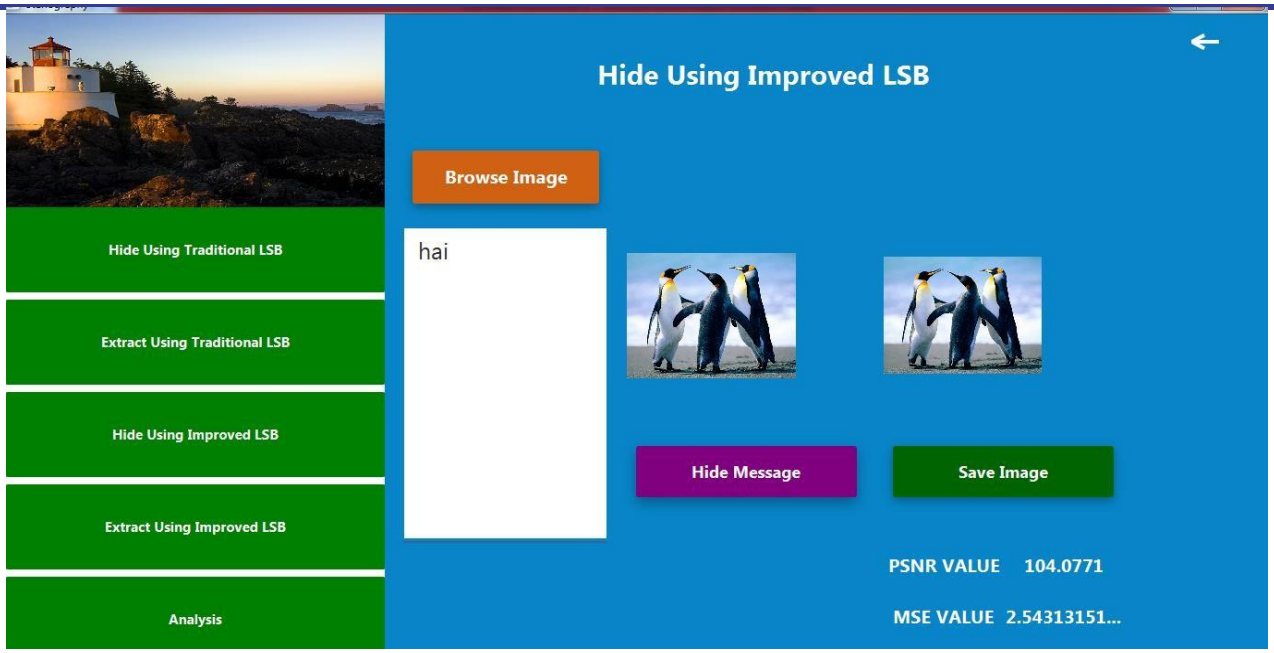

Figure 9. Screen Shot of Encryption Using Improved LSB Algorithm

5.2.6. Decryption of message using Improved Least Significant Bits

The bit where the message was hidden is first decoded and after it is determined, the message is decoded from the image. The decoded message is then decrypted by using a secret key.

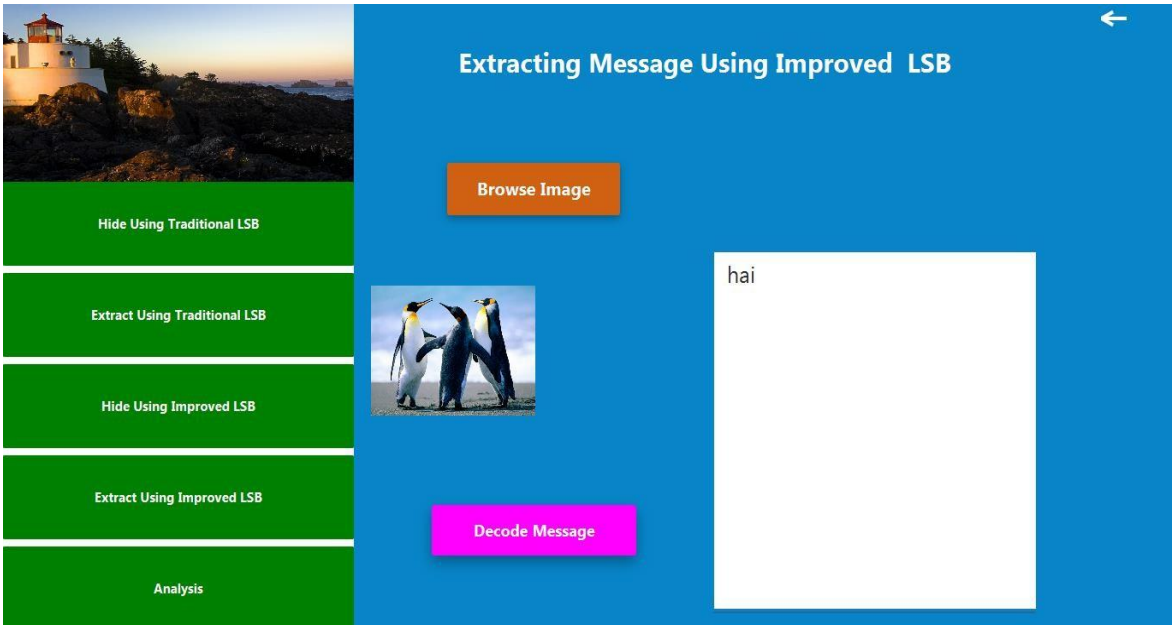

Figure 10: Screen Shot Of Extraction of Message Using Improved LSB

5.2.7 Simulation Phase

Traditional LSB Versus Improved LSB using PSNR parameter

After an image is selected and a secret message is hidden, the simulation phase compares the PSNR ratio value obtained when using the improved LSB method. The two values are plotted on a graph. Another graph plots the MSE value obtained when using the traditional LSB method versus the MSE value obtained when using he improved LSB method.

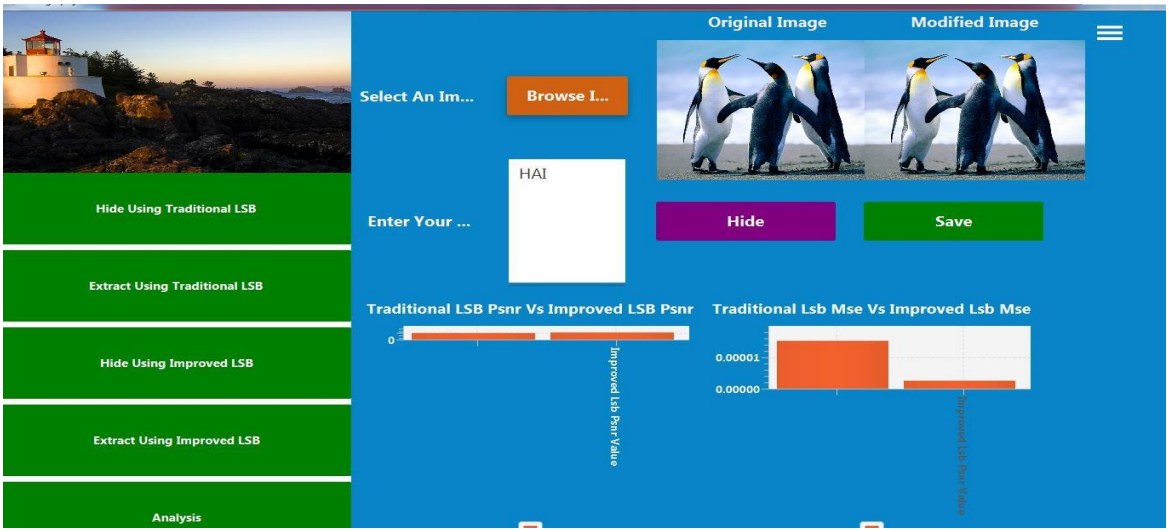

Figure 11: Traditional LSB Versus Improved LSB using PSNR and MSE Parameters

5.3. Experimental Design and Testing

An analysis to examine the statistical properties of the stego images produced by the proposed method and the traditional LSB method was carried out. PSNR and MSE image quality metrics were employed. A lower MSE value means a better image quality ie lesser distortion in the cover image while the higher the PSNR value the better the quality of the image. (Mei Jiansheng *et al* .2009).

Table 3. Test Data Images

File name	Dimensions	File Size
1.jpg	685x514 pixels	157 Kilo bytes
2.jpg	685x457 pixels	224 kilo bytes
3.jpg	685x457	161 kilobytes

The specific data hiding method which will ensure security was taken to be the independent variable (in this case the traditional LSB method and the proposed improved LSB method). In order to evaluate the efficiency of the proposed improved steganography method, the evaluation dependent variable all of which measure the image distortion levels were considered. Accordingly, for each steganography method (the traditional LSB method and the proposed improved LSB method) and for each cover image the value of each dependent variable was measured. The values of the dependent variables for both embedding methods were then compared.

5.3.1. Experimental Results

5.3.1.1. Peak Signal to Noise Ratio (PSNR)

Figure 7.0 shows the comparison of the PSNR of the three stego images for both the traditional LSB method and the improved LSB method. Every image tested registered a higher PSNR for improved LSB method as compared to the Traditional LSB method showing that the improved LSB embedding method distorts the image less improving on imperceptibility of the hidden data since a higher peak signal ratio to noise ratio (PSNR) indicates less distortion (Mei Jiansheng, 2009).

5.3.1.2. Mean Square Error (MSE)

Figure 8.0 shows a summary of the comparison of the MSE of three stego images for both the traditional LSB method and the improved LSB method. For each stego image, a lower MSE was recorded with the improved LSB method as compared to the traditional LSB method. A lower MSE value means a better image quality i.e lesser distortion in the cover image (Mei Jiansheng, 2009). This means that stego images generated by the improved LSB method have lesser distortions compared to those generated by the traditional LSB method and hence improved imperceptibility.

6.0 Conclusion

The study concluded that data transfer using the internet is growing fast, people, individuals and companies transfer documents. Security therefore becomes important especially when transferring the data because any unauthorized individual can hack the data and interfere with information. The also concluded that LSB is helpful since it offers effective information security mechanisms by implementing a two tier architectures which enhances security. Other benefits are improved sending of sensitive data via using improved steganography algorithm that is much harder to be intruded. In comparison to the traditional least significant bit algorithm, the method used in this research was found to demonstrate increased imperceptibility to attacks on the cover image. The hiding capacity which in turn ensures security can also be increased by varying the number of bits used per color channel. However the method is best suited for the purposes of communications applications as more permanent aspects like watermarking are not included in this research

7.0 References

Amirthajan, R. A. (2010). A comparative Analysis of image steganography. *International journal of computer application, 2*(3), 2-10.

Arora, P. R. (2015). Image Security System using Encryption and Steganography. *International Journal of Innovative Research in Science, iv*(06).

Ashiwini B, P. S. (2014). A hybrid approach for enhancing data security by combining encryption and steganography . *Proceedings of the international conference on advances in engineering and Technology*.

Atallah M. Al-Shatnawi. A (2012) New Method in Image Steganography with Improved image Quality.Journal ofApplied Mathematical Sciences, Vol. 6, No. 79, pp. 3907-3915,

Cox I.J, Miller J.M, & loom J. A. B (2002). *Digital Watermarking*. Morgan Kaufmann.

El-Hoby, H. M., Salah, M. A. F, & Suhaimi, M. A. (2014). Aligning Cloud Computing Security with Business Strategy. *International Journal of Computer Trends and*

Ettinger M (1998) "Steganalysis and game equilibria," in *Information Hiding, 2nd international Workshop* (D. Aucsmith, ed.), Lecture Notes in Computer Science, pp. 319–328, Springer.

Feldman, A. J. (2012). *Privacy and integrity in the untrusted cloud.* Mountain View, California, USA.

Grgic, M. (2001). Perfomance Analysis of image Compression using Wavelets. *ITIE , 48* (3), 682-695.

GundaSai Charnl, N. K. (2015). A Novel LSB based image steganography with multi level encryption. *2nd International Conference on innovations in information embedded and communication systems.*

International Conference on Issues and Challenges in intelligent Computing techniques.

International Journal Of Computer Science and Mobile Computing , 3 (5), 804-808.

International Journal of Engineering Trends and Technology , 3 (3).

Jajodia, N. J. (1998). Exploring Steganography: Seeing the unseeen. *IEEE Computer*, 26-34.

Karam, J. (2008). A New Approach in Wavelet Based Speech Compression. *Mathematical Methods, Computational Techniques, Non Linear Systems, Intelligent Systems*, 228-233.

Kumar R.P, Hemanth V.,(2015) "*Securing Information Using Sterganoraphy" International Conference on Circuits, Power and Computing Technologies (ICCPCT*), page(s): 1197 – 1200.

Maconanchy, C. S. (2001). A model for Information Assurance: An Intergrated Approach. *Proceedings of the 2001 IEEE Workshop on Information Assurance and security.* New York: U.S. Military Academy.

Meyyappan, R. N. (2012). Image Security using steganograpahy and cryptographic techniques.

Morkel, O. S. (2005). An Overview of Image Steganography. *Proceeding of the 5th annual information security.* South Africa.

Natasha T, D. P. (2015). Dual security: Proposed architecture. *International Journal of science,*

technology and Management , iv (02).

Pattewar, V. A. (2014). A novel Approach towards separable Reversible Data Hiding Techniques.

Prabakaran G, Bhavani R., Rajeswari P.S (2013), "Multi secure and robustness for medical image based steganography scheme" International Conference on Circuits, Power and Computing Technologies (ICCPCT), 1188 – 1193

Preet, R. G. (2014). A new proposed Practice for secure Image combining Cryptography, steganography and watermarking based on vaious parameters. *International Conference on contemporary computing and informatics.*

Rajkumar Y, Ravi S, and Kamaldeep. C (2011) Combination Method for Digital Image steganography with Uniform Distribution of Message. An International Journal on advanced Computing (ACIJ), Vol. 2, No. 6, pp. 29-43, November 2011.

Rashedul, A. S. (2014). An efficient filtering based approach improving LSB Image steganography using status bit along with AES cryptography. *3rd International Conference on Informatics, Electronics & Vision.*

Rengarajan A. Anushiadevi M. Kalpana D. & ohn B.B (2012) "*Seeable Visual But not Sure of It" IEEE-International Conference on Advances in Engineering, Science And management.*

Soni, P. B. (2012). A New approach of data hiding in images using cryptography and steganography. *International journal of computer application , 58* (18).

Tanuja, B. K. (2014). Enhance Two Tier Secure Model of Modern Image Steganography.

Technology (IJCTT)

Yung-Chen, C.-H. &. (2008). Digital invisible ink data hiding based on spread spectrum and quantization techniques. *IEEE transactions on multimedia, 10*(4).

Zoran D., Michael J., and Sushil J. (2010) Information Hiding: Steganography and steganalysis. *Review Article Handbook of Statistics*, Vol. 24, pp. 171-187, Katzenbeisser S.and Petitcolas F. A. P. (2010) Information Hiding Techniques for steganography and Digital Watermarking. Artech House Inc.