Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 04, April -2018

HIDING TEXT MESSAGES INTO IMAGES USING ADAPTIVE LEAST SIGNIFICANT BIT .

Increase in Security by Steganography

Mankirat Singh[1], Er.Jasdeep Maan[2]

[1]*Computer Science & Engineering, Bhai Maha Singh college of Engineering, Sri Muktsar Sahib*
[2]*H.O.D, Computer Science & Engineering, Bhai Maha Singh college of Engineering, Sri Muktsar Sahib*

Abstract —*Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier le formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points.*

Keywords-*Steganography, Cryptography, Fibonacci,*

I. INTRODUCTION

In present scenario, people exchange information with each other by means of various techniques such as cell phone or internet. But these techniques are not secure enough. As every person wants to keep their data about work to be secure and secret thus it is necessary to use such techniques that should provide security to both sender and receiver. Two techniques steganography and cryptography are helpful in the accomplishment of task for transferring and sharing of data in a secure manner. Sharing of data in concealed way is provided by these techniques. For a secure data communication, steganography and cryptography are popular concurrent techniques that provide security against human interception by operating data due to cipher or cover their existence. Cryptography provides encryption approaches for protecting data without damage and secure. In case of Cryptography person can tell that a message has been encrypted, but he can‟t decrypt the message without using the appropriate key. In steganography, message itself may not be difficult to decrypt but person would not detect the existence of message. When these both techniques are merging together provides two levels of security. Steganography has benefit over cryptography in hiding of secret transmission, where in cryptography the visibility of the secret information attracts the attention of wire tapper. Steganography is derived from the Greeks word “steganos” that defines covered writing. In ancient time, Greek used various methods to secure messages by writing a secret message on wooden tablets before concealing it with a fake writing on top of wax, or used to tattoo a message on a slave‟s head, then waiting for the hair growth for coverage then shave it back when it reaches the desired position. In present time, transmission of information in modern steganography systems is done secretly over public digital channels, within a bearer that appears to be nothing out of the normal.

1.1 STEGANOGRAPHY

Digital steganography is the art and science of hiding communications; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper’s suspicion. A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are still very limited methods of steganography to be used with communication protocols, which represent unconventional but promising steganography mediums. Digital image steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image steganography. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the stego image quality (imperceptibility).

RGB consists of 8 bits value per pixel representing 00000000 for the black pixels and 11111111 for the white pixels. While RGB (Red Green Blue) image consists of 24 bits values per pixel representing (00000000, 00000000, 00000000) and (11111111, 11111111, 11111111) for the white pixels. Red Green Blue (RGB) image is the most appropriate than other images because it contains large amount of data/information that will help in concealing the secret data/information with a bit variation in the image resolution (number of pixels in the image) and which doesn‟t lead to the distortion in the

quality of the image and make the message more secured. In this paper, image used is the RGB (Red Green Blue) as a message carrier to conceal the secret message by the LSB (Least Significant Bit) hiding technique as well as the proposed technique.

1.2 STEGANOGRAPHY AND WATERMARKING

Steganography aims to hide the very existence of communication by embedding messages within other cover objects. However, watermarking aims to protect the rights of the owners of digital media such as images, music, video and software. Even if people copy or make minor modification to the watermarked file, the owner can still prove it is his or her file. Thus, both of steganography and watermarking are forms of data hiding and share some common characteristics. Nevertheless, the goal of steganography is the embedded message while the goal of watermarking is the cover object itself. Watermarking is a data hiding technique that protects digital documents, files, or images against removal of copyright information. Even if someone knows that a watermark is exist (i.e. visible watermarking) in a given object, it should be impossible to remove the watermark from the watermarked object without causing a distortion or destroying the original (watermarked) object. This aspect or feature of watermarking is known as "robustness". According to the kind of embedded information, two techniques of document marking can be distinguished: watermarking and fingerprinting. Watermarking is the process of embedding a specific copyright mark into digital documents in the same way. On the other hand, in order to detect any break of licensing agreement, a serial number is embedded in every copy of this digital document. This process is known as "fingerprinting". Even if these markings are detected, it should be practically impossible to remove them.

1.3 STEGANOGRAPHY AND CRYPTOGRAPHY

Cryptography and steganography achieve separate goals. Cryptography conceals only the meaning or contents of a secret message from an eavesdropper. However, steganography conceals even the existence of this message (Lou and Liu, 2002). Furthermore, steganography provides more confidentiality and information security than cryptography since it conceals the mere existence of secret message rather than only protecting the message contents. Therefore, one of the major weaknesses of cryptosystems is that even though the message has been encrypted, it still exists.

Even though both cryptographic and steganographic systems provide secret communications, they have different definitions in terms of system breaking. A cryptographic system is considered broken if an attacker can read the secret message. However, a steganographic system is considered broken if an attacker can detect the existence or read the contents of the hidden message. Moreover, a steganographic system will be considered to have failed if an attacker suspects a specific file or steganography method even without decoding the message. As a result, this consideration makes steganographic systems more fragile than cryptography systems in terms of system failure. Additionally, steganographic systems must avoid all kinds of suspicion in order to achieve security and not be considered failed systems. Since steganography adds an extra layer of protection to cryptography, combining steganography and encryption gives the ultimate in private communication. Therefore, the purpose of steganography is to complement cryptography and to avoid raising the suspicion of system attackers but not to replace cryptography.

1.4 FIBONACCI SERIES

The Fibonacci numbers are the numbers in the following integer sequence, called the Fibonacci sequence, and characterized by the fact that every number after the first two is the sum of the two preceding ones:

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144,…

Often, especially in modern usage, the sequence is extended by one more initial term:

0 , 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144,…

By definition, the first two numbers in the Fibonacci sequence are either 1 and 1, or 0 and 1, depending on the chosen starting point of the sequence, and each subsequent number is the sum of the previous two.

The sequence F_n of Fibonacci numbers is defined by the recurrence relation:

$F_n = F_{n-1} + F_{n-2}$,
with seed values
$F_1 = 1, F_2 = 1$

or

$F_0 = 0, F_1 = 1.$

Fibonacci numbers appear to have first arisen in perhaps 200 BC in work by pingala on enumerating possible patterns of poetry formed from syllables of two lengths. The Fibonacci sequence is named after Italian mathematician Leonardo of Pisa, known as Fibonacci.

II. LITERATURE SURVEY

2.1 Increase of Quality and Size of Data in Steganography

Authors: Morteza Bashardoost, Ghazali Bin Sulong and Parisa Gerami et al. [2013]

The challenge of steganographic methods is to create a rational balance between the quality of the file and the size of data that can be transferred. In addition, the robustness of the technique and security of the obscure data are the facts that cannot be dissembled. The Least Significant Bit (LSB) insertion approach provides a high degree of visual quality and a large amount of capacity for the concealed data, but the covert message is not well protected in this method. In the proposed method, the secret data is firstly encoded by using the Vigenere encryption method to guarantee the protection of the hidden message. Afterward, the Lempel Ziv Welch (LZW) technique compresses the data to reduce the occupational capacity of the confidential data. Then, by utilizing the extended knight tour algorithm, each bit stream of the data is spread out on the image to increase the robustness of the method. The results show that the proposed method not only improves the security and payload capacity problems of the simple LSB method, but also increases the visual quality of the stego image.

2.2 Increase in efficiency

Authors: Ms.Soniya, Vijayakumar et al. [2013]

Steganography hides the text message in the bytes of the cover medium, which is the container, used to hide the message. Currently most of the steganography algorithms work by modifying the Least Significant Bit (LSB) of the consecutive bytes of the cover medium to store the secret data. The main drawback of this algorithm is that hidden message can be retrieved easily through steganalysis since the messages are stored in consecutive bytes. In this paper, two novel methods for selecting the bytes of the cover medium in which the secret data bits to be stored are proposed. In both methods, the byte of the cover medium where the secret data is to be stored is selected randomly. The first method is based on a linear polynomial function and the second method is based on a quadratic polynomial function. The present work compares the efficiency of the two methodologies.

2.3 Image Watermarking

Authors: Prabhishek Singh, R S Chadha et al. [2013]

This paper incorporate the detail study watermarking definition, concept and the main contributions in this field such as categories of watermarking process that tell which watermarking method should be used. It starts with overview, classification, features, framework, techniques, application, challenges, limitations and performance metric of watermarking and a comparative analysis of some major watermarking techniques. In the survey our prime concern is image only.

2.4 Security in Steganography and Digital Watermarking

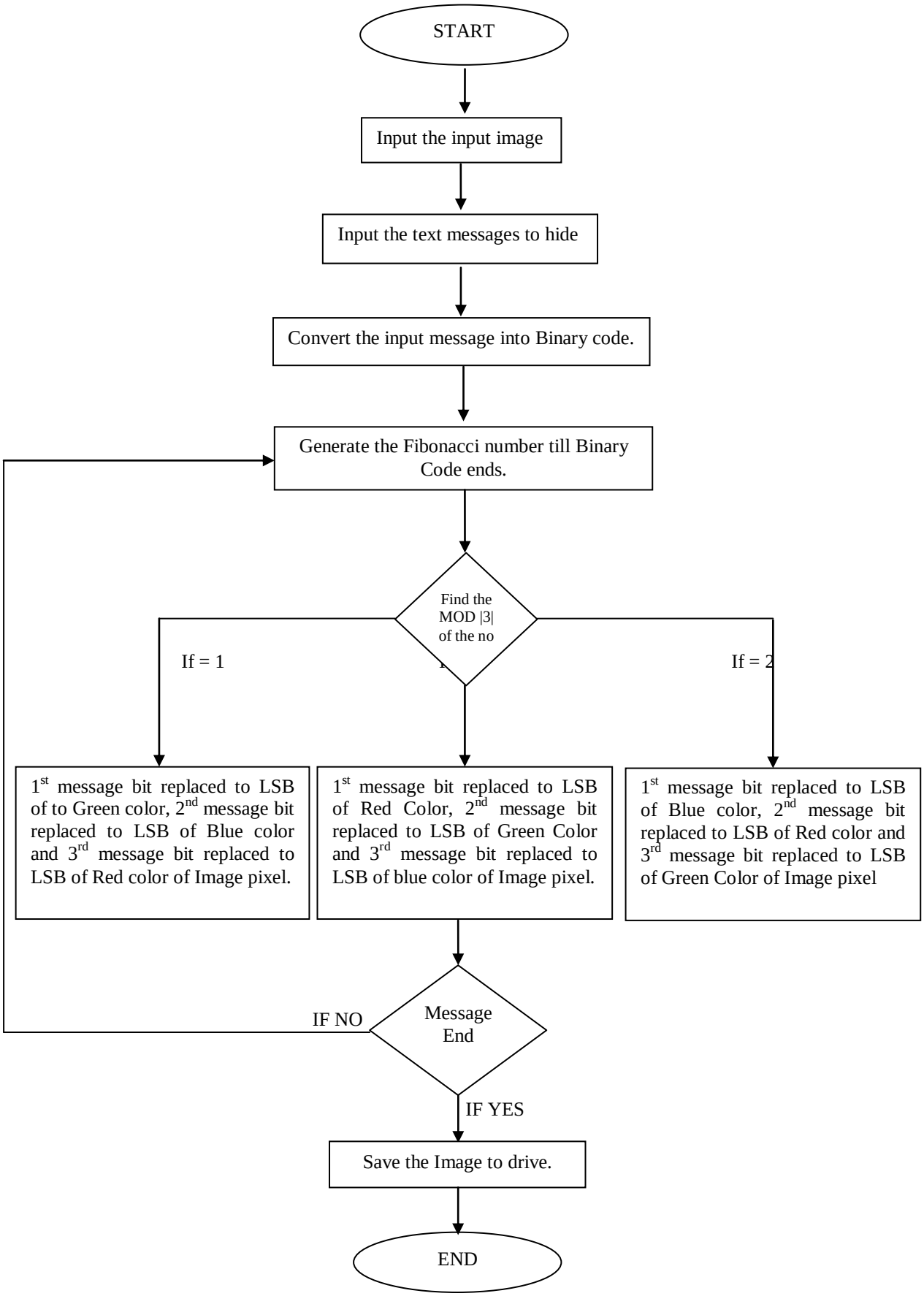
Authors: Ramadhan Mstafa, Christian Bach et al. [2013]

Innovation of technology and having fast Internet make information to distribute over the world easily and economically. This is made people to worry about their privacy and works. Steganography is a technique that prevents unauthorized users to have access to the important data. The steganography and digital watermarking provide methods that users can hide and mix their information within other information that make them difficult to recognize by attackers. In this paper, we review some techniques of steganography and digital watermarking in both spatial and frequency domains. Also we explain types of host documents and we focused on types of images.

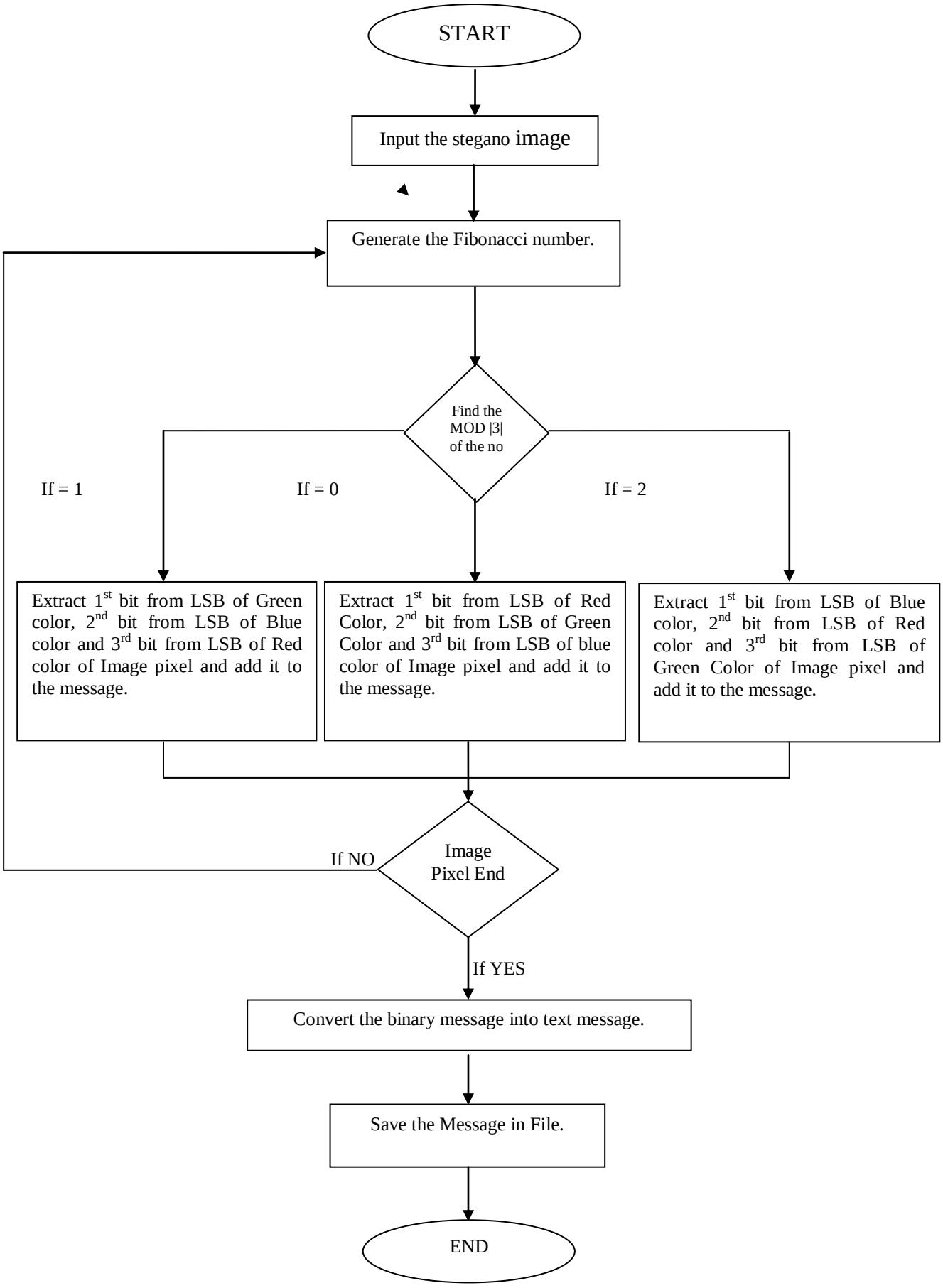
III. METHODOLOGY

The Proposed research aims to develop an improved steganography approach which is Adaptive LSB Method for color images with higher imperceptibility/quality, large capacity/payload and better in robustness/resistance to attacks. Images as well as text messages can be hiding within the images using sequential and random methods. It will incorporate cryptography to achieve high security and random pixel embedding to attain high immunity to attacks. It would be highly immune to any environmental disturbances like noise due to hybrid filtering.
The proposed system comprises of two components:

1. Embedding Module



2. Extracting Module.



V. RESULTS

Proposed system is tested on more than 50 images with different watermarks for data hiding. System is giving 94% accurate results.
PSNR (Peak Signal to Noise Ratio) of the obtained stego-image can be computed by

$$\text{PSNR} = 10\ log_{10} \frac{255^2}{MSE}$$

The results are then compared with various steganography methods as shown in the following table. In current work more pixel values is change because the simple LSB replacement depends upon size of image. Comparative study of previous method and adaptive LSB substitution method is shown below:

	Simple LSB		**Enhanced LSB**	
	Lena	**Baboon**	**Lena**	**Baboon**
Message Size (Bits)	65536	65536	651904	651904
PSNR	56.8745	56.9154	58.1958	58.2934
Accuracy	84.03 %	84.00 %	93.90 %	93.60 %

Table Comparison of the proposed system with the existing system

VI. CONCLUSION

There are several types of algorithms for stegnography. Each type of algorithms has its own advantages and limitations. No method can provide fully perfect solution. Each type of solution has robustness to some type of attacks but is less resilient to some other types of attacks. Main focus of the current research in this field is to make the stegnography algorithms resilient to geometric transformations. In case of practical application, choice of solution type actually depends on the nature of application and requirements. The proposed method uses Modified LSB Method to optimize the strength of steganographic process. The imperceptibility and robustness of proposed method shows better performance in comparison to other approaches in practice. Accuracy of the system evaluated to be 94% which shows considerably good improvement over the existing approaches.

REFERENCES

[1] Anant M.Bagade and Sanjay N.Talbar, *"A High Quality Steganographic Method Using Morphing"*, J Inf Process Syst, vol. 10, No.2, June 2014, pp. 256-270.
[2] Anupam Mondal, Shiladitya Pujari, "*A Novel Approach of Image Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients*", I. J. Computer Network and Information Security, vol. 3, 2015, pp. 42-49.
[3] Amit Singh, Susheel Jain, Anurag Jain, *"Digital watermarking method using replacement of second Least significant Bit(LSB) with inverse of LSB"*, International Journal of Emerging Technology and Advanced Engineering, vol. 3, Issue 2, February 2013, pp. 121-124.
[4] Chan-Il Woo and Seung-Dae Lee, *"Digital Watermarking for Image Tamper Detection using Block-Wise Technique"*, International Journal of Smart Home vol. 7, No.5, 2013, pp.115-124
[5] Gopika V Mane, G. G. Chiddarwar, *"Review Paper on Video Watermarking Techniques*", International Journal of Scientific and Research Publications, vol. 3, Issue 4, April 2013, pp. 1-5.
[6] Gurpreet Kaur, Kamaljeet Kaur, *"Image Watermarking Using LSB (Least Significant Bit)"* International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 4, April 2013, pp. 858-861.
[7] Henri Bruno Razafindradina and Attoumani Mohamed Karim, *"Blind And Robust Images Watermarking Based On Wavelet And Edge Insertion"*, International Journal on Cryptography and Information Security (IJCIS), vol. 3, No. 3, September 2013, pp. 23-30.

[8] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal, *"Text Steganography using Article Mapping Technique (AMT) and SSCE"*, Journal of Global Research in Computer Science, vol. 2, No. 4, April 2011, pp. 69-75.

[9] Jasleen Kour, Deepankar Verma, *"Steganography Techniques A Review Paper*", International Journal of Emerging Research in Management & Technology, vol. 3, Issue-5, 2014, pp. 132-135.

[10] Khosravi Sara, Abbasi Dezfoli Mashallah, Yektaie Mohammad Hossein, *"A New Stegnography Method Based On HIOP (HIGHER INTENSITY OF PIXEL) Algorithm and Strassen's Matrix Multiplication*", Journal of Global Research in Computer Science, vol. 2, No. 1, January 2011,

[11] Latika, Yogita Gulati, *"A Review of Steganography Research and Development*", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, Issue 4, 2015, pp. 871-874.

[12] Manpreet Kaur, Er. Amandeep Kaur, *"Improved Security Mechanism of text in Video by using Steganographic Technique: A Review"*, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, Issue 5, May 2014, pp. 216-220.

[13] Morteza Bashardoost, Ghazali Bin Sulong and Parisa Gerami, *"Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression"*, IJCSI International Journal of Computer Science Issues, vol. 10, Issue 2, No 1, March 2013, pp. 221-227.

[14] Ms. Soniya Vijayakumar, *"Image Steganography Based On Polynomial Functions"*, Journal of Global Research in Computer Science, vol. 2, No. 3, March 2011, pp. 13-15.

[15] Mr. Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, *"Image Steganography using Latest Significant Bit with Cryptography*", Journal of Global Research in Computer Science, vol. 3, No. 3, March 2012, pp. 53-55.

[16] Prabhishek Singh, R S Chadha, *"A Survey of Digital Watermarking Techniques, Applications and Attacks"*, International Journal of Engineering and Innovative Technology (IJEIT) vol. 2, Issue 9, March 2013, pp. 165-175.

[17] Rajat Tiwari, Navneet Kaur, Manpreet Kaur, *"An Optimization Image Watermarking Technique Using Biogeography Based Optimization"*, The International Journal of Engineering and Science (Ijes), vol. 2, Issue 3, 2013, pp. 64-70.

[18] Ramadhan Mstafa, Christian Bach, *"Information Hiding in Images Using Steganography Techniques, Information Hiding in Images Using Steganography Techniques*", ASEE Northeast Section Conference, March 14-16, 2013.

[19] Rashi Singh, Gaurav Chawla, *"A Review on Image Steganography*", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, Issue 5, May 2014, pp. 686-689.

[20] Rosziati Ibrahim and Teoh Suk Kuan, *"Steganography Algorithm to Hide Secret Message inside an Image"*, Computer Technology and Application, vol. 2, February 2011, pp. 102-108.

