e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

Secure Messaging Using Image Stegnography

Priyanka Sahute[1], Swati Waghamare[2], Supriya Patil[3],Ashwini Diwate[4]

[1234]Department of CSE, DACOE, Karad, 415110, India

Abstract: All important information can be send and receive over the network in secretly and safely by using image-steganography .The difficulty of existing system is that the intermediate person can easily hack the information that has transfer directly and also there is limitations in encrypted form. To make the security of information we are using Secure Messaging using Image Steganography. Any amount of data or document can be easily embedded. If any information is embedded in stego image and transfer to user without any disturbance of that cover image and intermediate person can't realized that secure information. RSA Algorithm & HASH-LSB technique has been used. In cryptography RSA Algorithm is used for Encryption & Decryption. RSA Algorithm having two approaches: Asymmetric & Symmetric. And in Steganography having different methods. In these Least Significant Bit (LSB) Method is used. It is simple approach for embedding message into image. Hash-function is used for find position of least significant bits of RGB pixels.

Keywords: Cryptography, RSA & HASH-LSB Algorithm, Steganography.

I. INTRODUCTION

Now a days there is a rapid development of the Internet and telecommunication techniques. Importance of information security is increasing. An application such as secret communication, copyright protection, etc, increases the need for research of information hiding systems[1]. Cryptography and Steganography are the major areas which work on Information Hiding and Security. The word steganography comes from the Greek "Seganos", which mean covered or secret and – "graphy" mean writing or drawing. Therefore, steganography mean, literally, covered writing [2]. One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered . In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images. The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged. on the internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography.

Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis. The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly .Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file 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 exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.

Image steganography is used to Provide security when sending file on internet[8]. The project implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file. In these way we have developed the software which is user friendly,Economy of scale, increase reliability[9].

II. LITERATURE REVIEW

There are large number of cryptographic and steganographic methods that most of us are familiar with RSA Algorithum and LSB insertion method. In RSA algorithum we can use the two prime number's .These two prime numbers used as a private and public key for encryption and decryption. In LSB technique adjusting the least significant bit pixels of the carrier image.

In existing system we can send the only message but can't send the any type of file or any business document. we can't send and receive the large amount of data. So it is not usefull for the real time applications. Hence there are limitations of existing system.

In existing system symmetric approach of RSA algorithum has been used so there are some limitations such as only limited amount of data can be encrypt as well as decrypt.

In these system when stego image will be created then it is realized that stego image will be disturbed as compare to the original image.Image steganography is the art of information hidden into cover image, Is the process of hiding secret message within another message[8]. Main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer. Today steganography is mostly used on computer with digital data being the carriers and networks being the high speed delivery channel [5]. Using steganography a secret message is embedded inside a piece of unsuspicious information and sent without anyone knowing the existence of the secret message. Secrets can be hidden inside all sorts of cover information that is text, image, audio, video, etc. Most steganographic utilities hide information inside image, as it is relatively easy to implement images are mostly used in the process or of steganography because it is hard to break[9].

There are various kinds of steganographic methods have been proposed. Image file for hiding the secret data is most useful as it can hide a large amount of secret data. The basic requirement of hiding a data in cover file and the relation of steganography with cryptography is discussed. The steganography is art of hiding data within the image file or image file. An Efficient Method for Steganography in image in which Secret Message is first encrypted by using cryptography algorithm

III. PROBLEM DESCRIPTION

Image Steganography is defined as the message or document can be transfer over the network secretly and securely. In this project we can embed the message as well as any type of file in stego image by using RSA and HASH LSB techniques. First of all the user select the cover image from the system. Then user write the message or browse the file from system they want. Then this message or file passed to the RSA algorithum for encryption purpose. When user passed message or file to the RSA algorithum then RSA generate the public as well as private key. Then these binary coded data as well as the cover image passed to the HASH LSB technique. When this data will be passed HASH LSB then this technique will be calculate the each RGB pixel value to the cover image. To sort out the LSB and MSB value of the image. We can change the only LSB value. When we can change only LSB value then original image will be doesn't disturbed. HASH LSB value calculate the LSB pixel value and insert into the message or file content in to the cover image and finally stego image will be created.

So by using the RSA (Symmetric) and HASH LSB technique we can implement the Secure messaging using the image steganography. When we can implement this system then we can embed the file or message easily in image format then there is no any change in original image. So intermediate person can't access the any secure data.

IV. IMPLEMENTATION

4.1 RSA Algorithm

RSA stands for Ron Rivest,Adi Shamir and Leonard Adlemann.who first publicly described the algorithm in 1977**.**RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.. A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message. Breaking RSA encryption is known as the RSA problem,whether it is as hard as the factoring problem remains an open question.

Generating Public and Private Keys

First, as we mentioned above, before any transmission happens, the Server had calculated its
public and secret keys. Here is how.

1.1) pick two prime numbers, we'll pick p = 3 and q = 11
1.2) calculate n = p * q = 3 * 11 = 33
1.3) calculate z = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 20
1.4) choose a prime number k, such that k is co-prime to z, i.e., z is not divisible by k.
We have several choices for k: 7, 11, 13, 17, 19 (we cannot use 5, because 20 is divisible by 5).
Let's pick k=7 (smaller k, "less math").
1.5) So, the numbers n = 33 and k = 7 become the Server's public key.
1.6) Now, still done in advance of any transmission, the Server has to calculate it's secret key.
Here is how.
1.7) k * j = 1 (mod z)
1.8) 7 * j = 1 (mod 20)
1.9) (7 * j) / 20 = ? with the remainder of 1 (the "?" here means: "something, but don't worry about it"; we are only interested in the remainder). Since we selected (on purpose) to work with small numbers, we can easily conclude that 21 / 20 gives "something" with the remainder of 1. So, 7 * j = 21, and j = 3. This is our secret key. We must not give this key away.
Now, after the Server has done the above preparatory calculations in advance, we can begin our message transmission.
Hence in this project we can use RSA algorithum for encryption and decryption purpose. By using RSA algorithm we can transfer the plaintext into the ciphertext means we get the binary coded format.

4.2 HASH BASED LSB TECHNIQUES

The image steganography takes the advantage of human eye limitation. It uses colour image as cover media for embedding secret message. The important quality of a steganographic system is to be less distortive while increasing the size of the secret message. In this paper a method is proposed to embed a colour secret image into a colour cover image. A 2-3-3 LSB insertion method has been used for image steganography.

PROPOSED HASH BASED LEAST SIGNIFICANT BIT 2-3-3 TECHNIQUE.

A hash based least significant bit technique is proposed. A colour image is considered as a cover media and secret data is embedded in this cover media as payload**.** The proposed technique takes eight bits of secret data at a time and put them in LSB of RGB (Red, Green and Blue) pixel value of the cover image in 2, 3,3 order respectively. Such that out of eight (08) bits of message five (05) bits are inserted in R and G pixel and remaining three (03) bits are inserted in B pixel. The detailed technique has been depicted in Figure 2(a) and (b). An illustration of the same is given in
section 4. This distribution pattern is taken because it is giving better results in terms of MSE and PSNR. The proposed method is not tested for the case of compressed images.

(a)

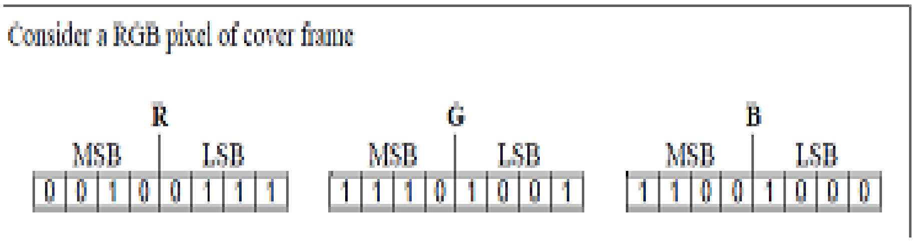

Fig.1.RGB pixel of cover image[1]

(b)

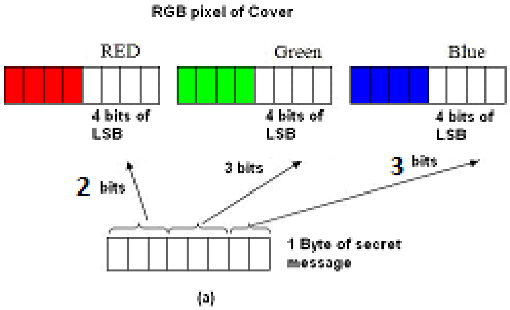

Fig.2.Calculete LSB of each RGB pixel value using HASH LSB[1].

Figure 2(a) and (b) An example of a cover pixel

Suppose 240 is value of secret image its binary value is 11110101 it is distributed in the order of 2 -3-3 to be embedded in LSB of RGB pixels respectively.

The hash function is as shown below,

_ _ _____ (1)

where, m is LSB bit position within the pixel, k represents the position of each hidden image pixel and l is number of bits of LSB which is 4 for the present case.

Let the hash function of Equation (1) return values m=1,2 for red, m=3,4,1 for green and m=2, 3, 4 for blue

So, after embedding the secret data in the particular pixel of cover image, The RGB pixel value of the stego image as below

00100111--------------Red

11101110--------------Green

11001011--------------Blue

The embedding positions of the eight bits out of the four (4) available bits of LSB is obtained using a hash function given in equation(1). The bits are distributed randomly using hash function which increases the security of the technique compared to other LSB based techniques [13, 14]. After embedding secret image in the cover image it will become a stego image. The intended user follows the reverse steps to retrieve the secret data. Using the same hash function which is known to the receiver, the data of the secret message is regenerated.

4.3 Steps for Encryption

1.Select image from the system.

2.Select or browse the message or file in system.

3.These secret message or file transfer to the RSA algorithm.

4.RSA perform the operation on that and generate the public and private key. By using RSA the

ciphertext will be created.
5.These binary data and cover image transfer to the HASH LSB technique.
6.HASH LSB performed the operation on that and to calculate the each RGB pixel value.
7.By using this LSB of RGB pixel value secure message or file will be transfer in to the cover image. So stego image will be created.
8.User send this message or file as well as private key to the receiver side.

4.4 Steps for Decryption

1.When receiver get the stego image and private key in zip format.
2.Then receiver extract this zip folder and passed stego image to the HASH LSB technique for decryption purpose.
3.Calculate the LSB of each RGB pixel value.
4.Then HASH performed on that and get the ciphertext.
5.This ciphertext and private key passed to the RSA algorithm for getting the original message or file.
6.RSA performed decryption by using private key and ciphertext and getting the plaintext means original message.
7.Like that finally receiver get the original message or file.

4.5 ARCHITECTURE DIAGRAM

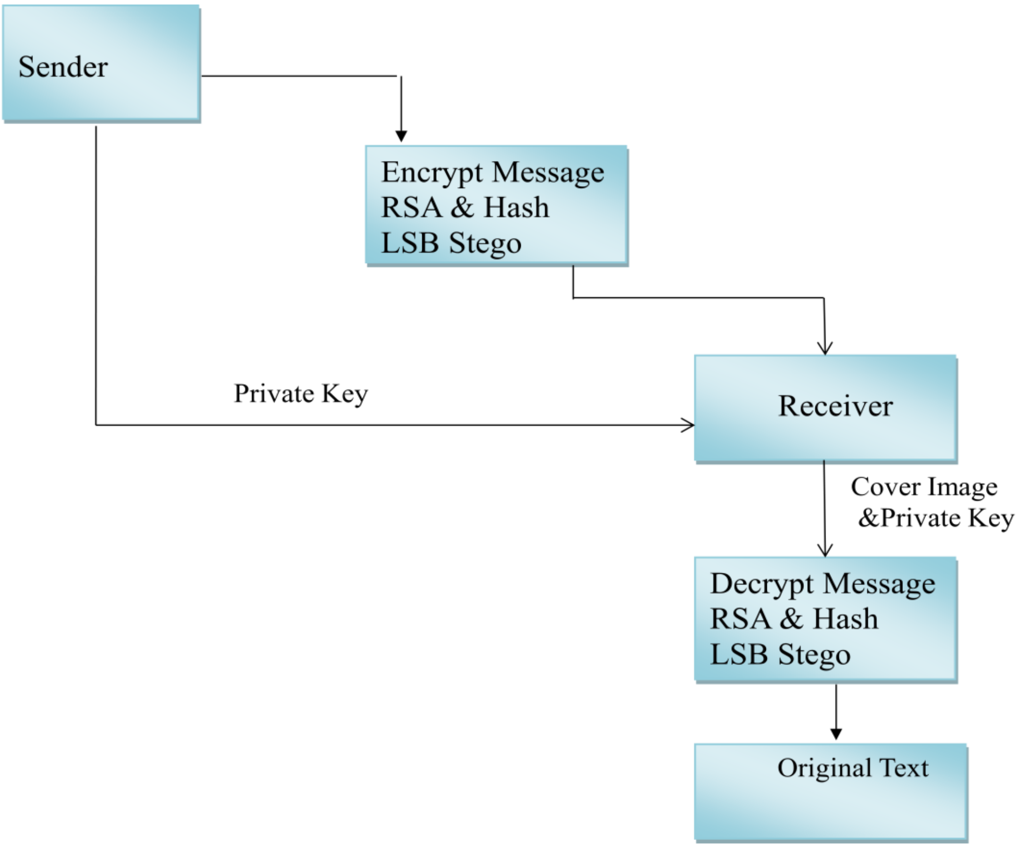

Fig.3.Architecture Diagram

In above fig.3 shows the Architecture dig of this system. In fig shows that sender send the secret message or file and cover image to the RSA algorithm and HASH based LSB technique. When RSA get the message or file then RSA generate the public and private key and ciphertext will be created. Then this ciphertext means binary coded value and cover image passed to the HASH LSB technique. By using this technique stego image will be created. Like that sender get the stego image and private key. Sender send this stego image to the receiver as well as private key also send to the receiver. The receiver side receiver get the original message or file by using RSA and HASH LSB technique.

V. RESULT AND DISCUSSION

In this project we can implement the one cryptography technique and one steganography technique. In steganography we can used HASH based LSB technique therefore original image will be does not change when we can convert into stego image. The result for all stego image using HASH LSB technique and original image have been compared which gives no changes will be done in both images. Hence in these way by using image steganography we can embed the message or file in to the cover image.

In fig shows the Test bed of Cover and Secret Images along with corresponding stego Images and Recovered Image.

Fig.a.Penguin.jpg

Fig.a.1 PenguiStego.jpg

Fig.b.Home.jpg

Fig.b.1 HomeStego.jpg

Fig.c.Day.jpg

Fig.c.1 DayStego.jpg

Fig.d. Lighthouse.jpg

Fig.d.1 LighthouseStego.jpg

Fig.e.Nature.jpg

Fig.e.1.NatureStgo.jpg

Fig.4.Fig.(a)-(e) 5 cover image and respective stego image.

In above all images shows that the cover image and stego image will be does not change, In fig.

Penguine.jpg shows that the cover image object while applying the RSA and HASH LSB technique we can embed the secret message in to that cover image and save these image as a penguinStego.jpg. when we can compared these both images we can realise that both image are same.
Like that in another image Lighthouse.jpg will be consider we can embed the file in that image and we get the stego image LighthouseStego.image. Again the both images are same.
So it is clear that we can embed the file or message in to the cover image by using Image Steganography method.

VI. CONCLUSION AND FUTURE DIRECTION

A secured Hash based LSB technique & RSA Algorithm for image Steganography has been implemented. We had transfer message and any type of file by using cryptography & steganography without any leakage of data or information. Though the file is large size it has been embedded in cover image without loss of data. RSA is a strong encryption algorithm that has stood a partial test of time. RSA implements a public key & private key cryptosystem that allows secure communication. In RSA Algorithm asymmetric approach has been used & in this approach public &private key are used. By using this approach communication between two users created successfully. To collect the RGB pixel values the LSB technique has been used. The data is encrypted by using RSA has been provided to HASH LSB then by using that LSB technique transfer data to cover image and then stego image is created. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

REFRENCES

[1]G.R.Manjula and AjitDanti," A NOVEL HASH BASED LEAST SIGNIFICANT BIT (2-3-3) IMAGE STEGANOGRAPHY INSPATIAL DOMAIN", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.

[2] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key", International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.

[3] Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.

[4] A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique Anil Kumar *, Markandeshwar University (MMU), Mullana, India Rohini Sharma Department of IT, M.M.E.C.,

[5]Computers and Society Encryption Algorithms Maharishi Chris Brooks, Department of Computer Science University of San Francisco

[6]Public-Key Cryptography and the RSA Algorithm, by Avi Kak (kak@purdue.edu)
April 23, 2014.

[7] Nentawe Y. Goshwe "Data Encryption and Decryption Using RSA Algorithm in a Network Environment "IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013 9 Manuscript received July 5, 2013 Manuscript revised July 20, 2013 .

[8]Palak R Patel, Yask Patel Survey on Different Methods of Image Steganography International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization)Vol. 2, Issue 12, December 2014.

[9] Palak R Patel, Yask Patel Survey2 on Different Methods of Image Steganography International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization)Vol. 2, Issue 12, December 2014.

[10] Prof. Dr. P. R. Deshmukh , Bhagyashri Rahangdale, Bhagyashri Rahangdale," Hash Based Least Significant Bit Technique For Video Steganography " Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 1(Version 3), January 2014, pp.44-49.

[11] Avi Kak (kak@purdue.edu),"Public-Key Cryptography and the RSA Algorithm" March 24, 2015c, 2015 Avinash Kak, Purdue University.

[12] Anil Kumar *, Rohini Sharma**,** "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering © *2013, IJARCSSE All Rights Reserved Page | 363* ,Volume 3, Issue 7, July 2013 ISSN: 2277 128X**.**

[13**]** Deepesh Rawat, Vijaya Bhandari, "*A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image*", International Journal of Computer Applications, Vol. 64, Issue No. 20, Feb., 2013.

[14]

Ankit Chaudhary, J. Vasavada, J. L. Raheja, S. Kumar, M. Sharma, "*A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images*", 22nd International Conference on Computer Graphics and Vision, 2012.

[15] R. Amirtharajan, R. Akila, P. Deepika chowdavarapu, "*A Comparative Analysis of Image Steganography*", International Journal of Computer Applications, Vol. 2, Issue No. 3, May, 2010.

[16] Samir Kumar Bandyopadhyay, Sarthak Parui, "*A Method for Public Key Method of Steganography*", International Journal of Computer Applications, Vol. 6, Issue No. 3, Sept., 2010.

[17] P. Nithyanandam, T. Ravichandran, N. M.Santron, E. Priyadarshini, "*A Spatial Domain Image Steganography Technique Based on Matrix Embedding and Huffman Encoding*", International Journal of Computer Science and Security (IJCSS), Vol. 5, Issue No. 5, 2011.

[18] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong-Yee Lee, "*A High Capacity 3D Steganography Algorithm*", IEEE Transactions on Visualization and Computer Graphics,Vol. 15, Issue No. 2, Pages No. 274 – 284, March-April, 2009.

[19] Jing-Ming Guo, Thanh-Nam Le, "*Secret Communication Using JPEG Double Compression*", Signal Processing Letters, IEEE, Vol. 17, Issue No. 10, Pages No. 879 – 882, Oct., 2010.

[20] Ross J. Anderson, Fabien A. P. Petitcolas, "*On the Limits of Steganography*", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481, May, 1998.