ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

Secure Image Transmission Technique using Cryptograhy and Steganography

[1] A. Poonguzhali , [2] Bindhiya B.S , [3] Dhanvanthi P , [4] Deeksha V, [5] Chaithra S
[1] Assistant Professor, [2],[3],[4],[5] UG Scholars
Department of Electronics and Communication Engineering
Sri Sairam College of Engineering, Anekal, Bengaluru-562 106

Abstract: **Cryptography and steganography are two conventional techniques used to cipher or hide information or data in existing communication. Cryptography is the art of saving information by encrypting it into an obscure format. On the other hand, steganography is the art and science of secret communication to send messages in a way which hides even the existence of the communication. Although cryptography and steganography provide an acceptable level of security when used separately via communicating in the unreliable medium like the Internet, advances in steganalysis make it a constantly an evolving field. This project aims to improve a new scheme of hiding a secret image in a cover image, by exploiting the benefits of combining both cryptography and steganography.The security of the images has always been a concern while transferring the images over the internet. In the proposed framework, the secret Image is encrypted using XOR Cipher Algorithm and embedded into the cover image using LSB Algorithm.Finally the encrypted secret image file is extracted from embedded cover image using LSB algorithm and decrypting the secret image again using Stream cipher algorithm to recover the original image.**

I. INTRODUCTION

Day by day, the use of internet has increased all over the world. Because of the increasing demand for information security, image encryption decryption has become an important research area and it has broad application prospects. The field of encryption is becoming very important in the present era. Image security is of utmost concern as web attacks have become more and more serious.

The huge amount of data and images are available for daily communication over the internet. Even the secret data can be transferred by hiding into images over the internet. So there is a need to provide security by means of authentication to this important data and images. In this regard, the file containing data, in encrypted images has lot of importance. Data hiding is a technique to embed additional messages into some distortion-unacceptable cover media, such as military or medical images; so that the original cover content can be perfectly restored after extraction of the hidden message file. This technique is also called as lossless, distortion free, or invertible data hiding technique.

II. LITERATURE REVIEW

2.1 Why Data Hiding?

As the technology has increased day by day the usage of multimedia, web documents and images has also increases on the network. Large amount of images are transferred on the internet every day, so it's necessary to provide security to these images from the hackers. It may happen that the hackers may capture the images, view the important contents and after viewing the contents they can modify the images and send it to destination. So the original image contents will be modified and the receiver can be totally unaware from this fact. Due to this, a small amount of distortion has occurred. Such distortion is not acceptable in some applications, such as medical imaging or in military images etc., because it may lead to risks of incorrect decision making. From this point of view a data hiding technique, which is referred to as reversible, invertible, lossless, or distortion-free, has been developed in recent years. In this review, data hiding methods which produces stego images with good qualities and high data hiding capacities are proposed. The data hiding techniques can be implemented to restore the hidden data after the original image has been extracted out.

2.2 Need for the system

Because of the increasing demand for information security, image encryption decryption has become an important research area and it has broad application prospects. The field of encryption is becoming very important in the present era. Image security is of utmost concern as web attacks have become more and more seriousTo make the data secure from various attacks and for the integrity of data they must encrypt the data before it is transmitted or stored. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), product, financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer. If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, than such a breach of security could lead to declination of war, wrong

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

treatment etc. Protecting confidential images is an ethical and legal requirement. Another use of network (World Wide Web) could be for sending secure data
which may be very essential for a group of companies, which should not be viewed by others. Therefore sensitive data hiding becomes most important area in securing network data.

Table 2.1 LITERATURE SURVEY COMPARISON TABLE

Paper	Authors, year	Technique Used	Advantages	Drawbacks
Improving various reversible data hiding schemes via optimal codes for binary covers,	W. Zhang, B. Chen, and N. Yu2012	Used a decompression algorithm as the coding scheme for embedding data.	The proposed code Construction is proved to be optimal when the compression algorithm reaches entropy.	It only use two simple methods to modify HS, and therefore, the problem is whether there exists other more effective modifying methods or not. Another problem is how to design recursive codes for gray scale covers.
Reversible Data Hiding Principles, Techniques, and Recent Studies"	Noorul , Rounak Kareem Mehdi Hanni 2011	primary techniques as the principles of RHD are talked. Pairwise logical computation data hiding technique (PWLC) and Data hiding by template ranking with symmetrical Central pixels(DHTC) technique.	Here investigated some RDH techniques. Also discussed their advantages and disadvantages	There will be no idea about which is suitable in which domain
Reversible image watermarking using interpolation technique	Lixin Luo, Zhenyung Chen, Ming Chen, Xiao Zeng, and Zhang Xiong 2010	It utilize the interpolation-error, the difference between interpolation value and corresponding pixel value, to embed bit "1" or "0" by expanding it additively or leaving it unchanged	which can embed a large amount of covert data into images, and achieves better image quality The computational cost of the scheme is small.	Any mistake in the calculation of interpolation will effect the secret information
"Reversible watermarking algorithm using sorting and prediction,"	V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi 2009	sorting technique is used to record the prediction errors based on magnitude of its local variance.	the proposed scheme can embed more data with less distortion.	More calculations are needed Size of location map affects the efficiency of the system
An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding"	T. Bhaskara Reddy, Miss. Hema Suresh Yanguani , Mr.T. Sri Harish Reddy, S. Karan 2013	This algorithm is based on Ceaser Cipher algorithm, random generation technique, concept of shuffling the rows i.e. rows transposition and Huffman Encoding.	provides high security to an image and occupies minimum memory space.	Some problems in the decoding section such that , here Huffman coding is used
"Reversible Data Hiding With Optimal Value Transfer"	Xinpeng Zhang 2013	the optimal rate or value modification under a payload-distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed	the optimal transfer mechanism gives a new role of value modification and can be used on various cover values	computation complexity due to the prediction will be higher
Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach	Subhasya R.J (1), Arpana Dayananda N (2)" 2014	uses the watermarking algorithm that embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square distortion between the original and watermarked image and also to increase Peak signal to noise ratio.	can improve the quality of the watermarked image and give more robustness of the watermark and also increasing PSNR	Low hiding capacity and complex computations
"Separable reversible data hiding in encrypted image."	Y. Zhang, 2012	a novel scheme for separable reversible data hiding, which consists of image encryption,data embedding and data-extraction/image-recovery phases.	Simple Less computation	Data compression is not efficient

2.3 Existing System

In past times,method used was humans, wax tablets and invisible ink, which in modern society totally changed. Now a day's images, pictures, videos and voices are used as a carrier, they transferred from one place to other with the help of telecommunication network.
There are many image encryption algorithms which are available such as Baker's Transformation, in this Baker's map is used for image encryption; Magic cube transformation is used to scramble the image pixels etc.But all these have some disadvantages for that purpose new algorithm has been developed in recent years.

1.Data encryption standard (DES)

DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team around 1974 and adopted as a national standard in 1997. DES is a 64-bit block cipher under 56-bit key. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation. DES application is very popular in commercial, military, and other domains in the last decades. Although the DES standard is public, the design criteria used are classified. There has been considerable controversy over the design, particularly in the choice of a 56-bit key.

2. Triple des (TDES)

The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching. TDES uses three round message this provides TDES as a strongest encryption algorithm since it is extremely hard to break 2^168 possible combinations. Another option is to use two different keys for the encryption algorithm. This reduces the memory requirement of keys in TDES. The disadvantage of this algorithm is that it is too time consuming.

3. Advanced encryption standard (AES)

AES was developed by two scientists Joan and Vincent Rijmen in 2000. AES uses the Rijndael block cipher. Rijndael key and block length can be 128, 192 or 256-bits. If both the key-length and block length are 128- bit, Rijndael will perform 9 processing rounds. If the block or key is 192-bit, it performs 11 processing rounds. If either is 256-bit, Rijndael performs 13 processing rounds.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

4. RSA algorithm

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The technologies are part of existing or proposed Web, Internet, and computing standards.

III. DESIGN METHODOLOGY

3.1 Proposed System

A combination of both steganography and cryptography has been tried.But the main focus was on encrypting the image file and hiding the image file. In this paper an attempt has been made to combine the most effective algorithms for steganography and cryptography to secure the secret images. The method used in this project combines the image steganography algorithm, Least Significant Bit (LSB) and the cryptographic algorithm, XOR Cipher. XOR Cipher Algorithm has been used to encrypt and decrypt the secret-image. XOR Cipher has been proved to be the best among the many cryptographic algorithms and has stood the test of the time. LSB is a common algorithm used for steganography and is comparatively efficient than many other algorithms. A combination of these too could offer a very powerful security method and the same has been experimented.

3.2 Proposed Algorithms

In the proposed method, a combination of steganography and cryptography has been applied. The following are the proposed algorithms used in this project.

3.2.1 XOR Cipher Algorithm

A **stream cipher** is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream).

In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as ***state cipher***. In practice, a digit is typically a bit and the combining operation an exclusive-or (XOR).

The pseudorandom keystream is typically generated serially from a random seed value using digital shift registers. The seed value serves as the cryptographic key for decrypting the ciphertext stream.

Exclusive-OR (XOR) encryption is an encryption method that is hard to break through with so called “brute force” methods.

Creating Keys

A symmetric Encryption key is used for this algorithm, which means the same key is shared for both Encryption and decryption. In this step, we define the algorithm for generating key for encryption and decryption process. The key generation algorithm is based on pseudorandom number generation concept.

In algorithm we pass a number of bytes n as input for key generation. The program generates n number of random number which is treated as secret key. These secret keys are then converted to bits for performing cryptographic operations.These secret keys are shared by only sender and receiver.

Encrypting/Decrypting the Image

In the image encryption part, we pass a secret image and secret keys as input to the function file. The function file calculates the length and breadth of secret image. It performs an XOR operation between pixels values of secret image and binary values of generated key values. After performing XOR operation between pixels values of secret image and binary values of secret keys, the input image is converted into encrypted image i.e.; no one can identify original image without the knowledge of secret keys.

In the decryption part, we pass the encrypted image and secret keys as input to the function file. Again the function file performs XOR operation between pixels values of encrypted image and secret keys which results as original input image as aim of cryptography approach.

3.2.2 LSB Algorithm

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding image in an image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8^{th} bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed. We use LSB substitution for embedding the image in an image.

4 bit data hiding method

Each pixel contains 8 bits, the right most bit is Least Significant Bit (LSB) and left most bit is (Most Significant

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

Bit) MSB. Four bit data hiding method, which embeds first four MSB bits (MSB,MSB-1,MSB-2,MSB-3) of secret image into last four LSB bits (LSB, LSB+1, LSB+2,LSB+3) of cover image. So last 4 bits of cover image is replace with first four bits of secret image.

Now next pixel of cover image is taken and again 4 MSB bits of next pixel of secret image is inserted into 4 LSB bits of cover image.

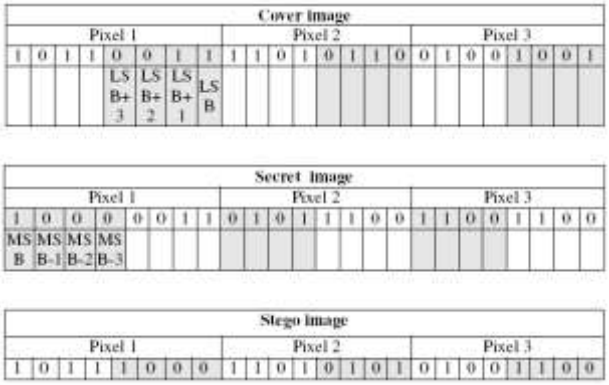
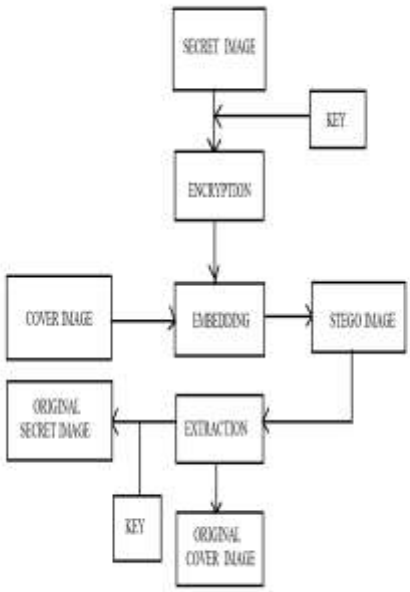


fig3.1 Data hiding process using 4 bit method

3.3 Block Diagram



3.4 Advantages

1.Capable of hiding secret image into the image.
2.Better recovered image quality
3.Very low distortion

3.5 APPLICATIONS

1.Internet communication,
2.Multimedia systems,
3.Medical Imaging,
4.Telemedicine,
5.Military communication, etc.

IV. SOFTWARE USED

MATLAB (**mat**rix **lab**oratory) is a numerical computing environment and fourth-generation programming language. Developed by MathWorks, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and Fortran.

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems.

In 2004, MATLAB had around one million users across industry and academia.MATLAB users come from various backgrounds of engineering, science, and economics. MATLAB is widely used in academic and research institutions as well as industrial enterprises.

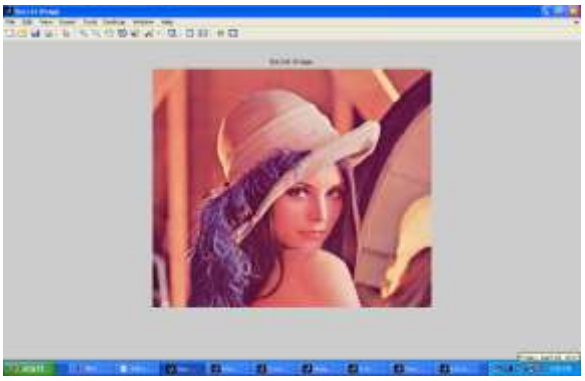
V. IMPLEMENTATION RESULTS

The proposed system consists of three phases: **Phase-I:** Image Cryptography – XOR Cipher Algorithm
Phase-II: Image Steganography - Least Significant Bit Algorithm
Phase-III: Image Extraction/Image Recovery using Cryptography and Steganography

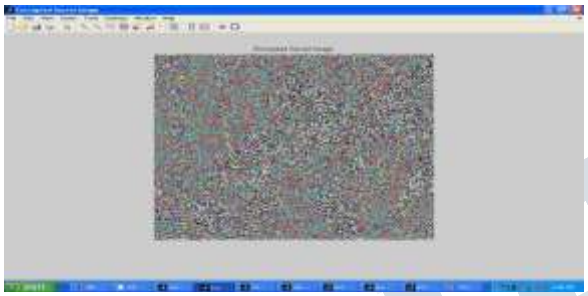
5.1 Phase-I:

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017



Secret Image to be Hidden



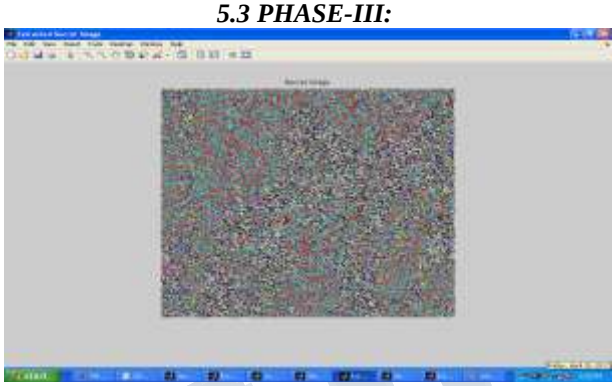
ENCRYPTED SECRET IMAGE TO BE HIDDEN

5.2 PHASE-II:

ORIGINAL/COVER IMAGE

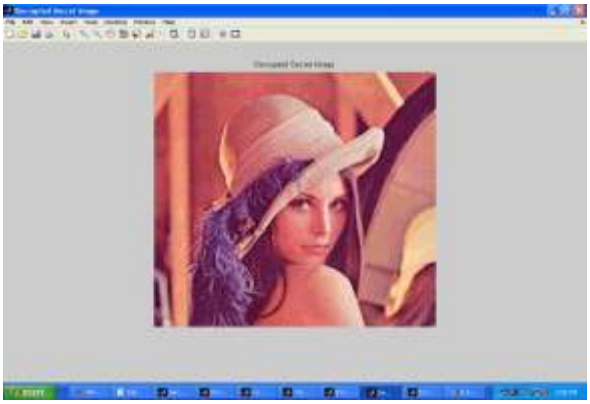
LSB -STEGO IMAGE

5.3 PHASE-III:



DECRYPTED SECRET IMAGE FROM STEGO IMAGE

RECOVERED COVER IMAGE FROM STEGO IMAGE



DECRYPTED /RECOVERED SECRET IMAGE

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

5.4 CONCLUSION

In this project an attempt was made to combine both steganography and cryptography. **T**he main *advantage* of stream *ciphers* is their high speed for both *encryption* and decryption. The advantages of LSB are its simplicity to embed the bits of the secret image directly into the LSB plane of cover-image. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB. Experimental results show that both the algorithms used offers high quality images. Thus combining cryptography with steganography offers an ideal system for secret data transmission with higher consistency with respect to stand-alone cryptographic techniques. Thus this scheme provides two tier securities, first using cryptographic key and second using stego key where the secret message is encrypted before embedding and decrypted after decoding. The extracted secret image or secret data is perceptually similar to the original secret image or data. Hence, an unintended observer will not be aware of the very existence of the secret-image.

5.5 FUTURE SCOPE

The huge amount of data and videos are available for daily communication over the internet. Even the secret data can be transferred by hiding into videos over the internet. So there is a need to provide security by means of authentication to this important data and videos. In this regard, the file containing data, in encrypted videos has lot of importance. Data hiding is a technique to embed additional messages into some distortion-unacceptable cover media, such as military or medical videos; so that the original cover content can be perfectly restored after extraction of the hidden message file. This technique is also called as lossless, distortion free, or invertible data hiding technique.

REFERENCE

1. “Expansion Embedding Techniques for Reversible Watermarking”,By Diljith M. Thodi and Jeffrey J. Rodríguez - in IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 3, MARCH 2007

2.” Efficient Compression of Encrypted Grayscale Images”,By Wei Liu, Wenjun Zeng,Lina Dong, and Qiuming Yao – in IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 19, NO. 4, APRIL 2010

3.” An Efficient Buyer-Seller Watermarking Protocol Based on Composite Signal Representation”,By M. Deng, T. Bianchi, A. Piva, and B. Preneel – in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18

4.”Reversible Image Watermarking Using Interpolation Technique”,By Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong – in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 1, MARCH 2010

5. “Scalable Coding of Encrypted Images”, By X. Zhang, G. Feng, Y. Ren and Z. Qian – in IEEE Trans. Inform. Forensics Security, vol. 21, no. 6, pp.3108-3114, June 2012.

6. “On compressing encrypted data”,By M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, -in IEEE
Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

7."Expansion Embedding Techniques for Reversible Watermarking”,By D. M. Thodi and J. J. Rodriguez – in IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 3, MARCH 2007

8. “Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification”,By Z. Qian, X. Han and X. Zhang – in 3rd International Conference on Multimedia Technology (ICMT 2013), pp. 869-876, Guangzhou, China, 2013.