INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Robust security approach using hybrid steganography

Pranay Kapgate
pranaykapgate01@gmail.com
Shram Sadhana Bombay Trust's College of Engineering, Jalgaon, Maharashtra

Surendra Demgunde
surendrademgunde@gmail.com
Shram Sadhana Bombay Trust's College of Engineering, Jalgaon, Maharashtra

Nikhil Tulankar
tulankarnikhil9@gmail.com
Shram Sadhana Bombay Trust's College of Engineering, Jalgaon, Maharashtra

ABSTRACT

Information security is one of the major problem faced nowadays since the number of internet users are increasing and secret information is getting shared every second. This has also hiked the cyber-crime and threat of malicious access. The two main techniques that are used for information security are steganography and cryptography. Cryptography can be basically considered as secret writing; on the other hand, Steganography can be considered as data hiding. In this project, a hybrid technique for data security is proposed by combining the cryptography and steganography properties. The proposed image steganography algorithm works on improvement of data embedding capacity. Implementation of image processing is implemented using modified LSB approach which showed improved results in terms of image quality and data hiding capacity. The aim of this work is to implement a system for data security as well as improve the data hiding capacity. The results show increased image quality and fewer distortions. Also proposed key exchange protocol will aid in security.

Keywords: *Security, Cryptography, Steganography, Hybrid Technique, Protocol.*

1. INTRODUCTION

The extensive growth of the internet in the last several years is leading the trend of high data consumption by the people. Users of the internet are consuming the digital data in massive quantities. As some security measure, cryptography techniques are used, but today use of cryptography as the only measure of security is inadequate for information security. To better handle, the problem of security steganography can be used. Steganography is the art of hiding the data in its entirety, unlike cryptography which scrambles the data to obscure its meaning. Steganography is a word from Greek origins which converts into covert writing. Steganography covers a wide range of methods for secret communication that hide or cover the very existence of the secret message. Some of these methods are digital signatures, watermarking, character arrangement, and invisible ink [1]. Many approaches for steganography are proposed in the recent years [2]. The most common approach to implementing steganography is by replacing Least Significant Bit (LSB) of the pixels with the message bits [3] [4].

In this paper, a combined approach for steganography and cryptography is proposed which combines LSB based steganography scheme with AES encryption for further improvement in security. Also, a secure key exchange protocol using RSA encryption is proposed for the overall gain in security. The proposed approach is secure, reliable, and provides better image quality.

2. LITERATURE REVIEW

Amrit Pal Singh et al. [4] developed an improved method for image steganography using LSB technique. This worked by slicing the three planes of RGB image and then hiding the data into each plane based on color sensitivity by using LSB technique. It resulted in high embedding capacity and better image quality. Its PSNR value was better than previous steganographic methods.

V. Lokeswara Reddy et al. [5] focused on BMP uses lossless compression, LSB makes use of BMP image. To be able to hide a secret message inside a BMP file, one would require a very large cover image. BMP images of 800x600 pixels found to have fewer web applications. Moreover, such uses are not accepted as valid. The proposed technique can be used for hiding images in 24-Bit, 8-Bit format. For this reason, LSB Steganography has also been developed for use with other image file formats.

Dr. D. Samidha et al. [6] described several techniques of image steganography in the spatial domain. Along with existing techniques like LSB, layout management schemes and replacing only l's or only zero's, some more methods like replacing intermediate bit,

raster scan principle, random scan principle, color based data hiding and shape based data hiding are also proposed. These new techniques are based on random selection of pixels for data hiding considering many parameters of an image like physical location and the intensity value of the pixel, etc.

Sourabh Chandra et al. [7] proposed a symmetric key cryptographic algorithm which is content based. This algorithm included binary addition operation for encrypting the plain text and circular shift operation and folding method for making the key secure. This algorithm posed a difficulty for the opponent to decrypt the key and text.

R. Samant et al. [8] proposed a method which does not only provide a better way for embedding large amounts of data into cover images with imperceptions, but also offers an easy way to accomplish secrecy. Basically, it tries to embed more data into the rough part of the image so that the distortion caused will not be visible. This method provides better results as compared to LSB replacement method where the distortions are spread all over the image. The images used for this algorithm are only 8-bit gray level images to avoid the further complications.

3. METHODOLOGY

Advanced Encryption Standard Algorithm (AES)

The AES is Advanced Encryption Standard Which is symmetric block Cipher. The AES Algorithm is used to encrypt important data. In AES algorithm same key used for Encryption and Decryption. The AES works on the principle of Substitution and Permutation. In AES the block size is 128 bits are arranged in such manner forms 4 x 4 matrix and key size is 128 bits, 192 bits, and 256 bits. In our project, we use AES algorithm to encrypt the message using symmetric key, before hiding into the image. So the output will be encrypted string or message.

Modified Least Significant Bit (Modified LSB)

In Modified LSB approach the data or secret message hidden inside image. We take sensitive data which we want to communicate, then this data is encrypted by AES algorithm. It gives encrypted data, this encrypted data is converted into binary code.

Take the cover image in which we want to encode data. The image is made up of pixel and pixel is having Red (R), Green (G), and Blue (B) values. Each value is 8 bit long. Then RGB having 24 bits. Steganography procedure is to be modified by simple LSB technique with little modification as, Instead of using only the last bits of the 24-bits in the pixel, 2 LSB bits are changed for storing the data.

Example, Cover Image pixels are,

10010101 11100011 01110010 01111111

And suppose data we want to hide: 10101100

Then, Stego Image Pixels will be like,

10010110 11100010 01110011 01111100

Split the image into RGB of 24 bits and modify last two bits of each pixel with an encrypted message which is already converted into binary code. By doing this the pixel is modified but human eye can't detect this. So data is encoded inside the image.

In decoding after decoding image and binary code is obtained, then this binary code is converted into string and pass to AES decryption algorithm.

Example, Stego Image Pixels,

10010110 11100010 01110011 01111100

Cover Image pixels are,

10010101 11100011 01110010 01111111

Data we get,

10101100

Binary Code is converted into Encrypted message or string, by using the symmetric key it decrypts the message and we get a secret message.

Example, Binary Code,

10101100

Key Exchange Protocol

The AES algorithm having a symmetric key for encryption and decryption. So as well as the encoded image we want to share symmetric key for decrypt message and this is not a secure way to share a key, we using key exchange protocol mechanism in which the client request for a key to server and server gives public key, by using the public key the client encrypts the AES key. This is done using RSA algorithm. This encrypted key is share to another client. Another client decode image then for decryption it requires AES key, client 2 having Encrypted AES. Client 2 request server for the private key then server gives private key to client 2. By using private key client decrypts the AES key and decrypts the message.

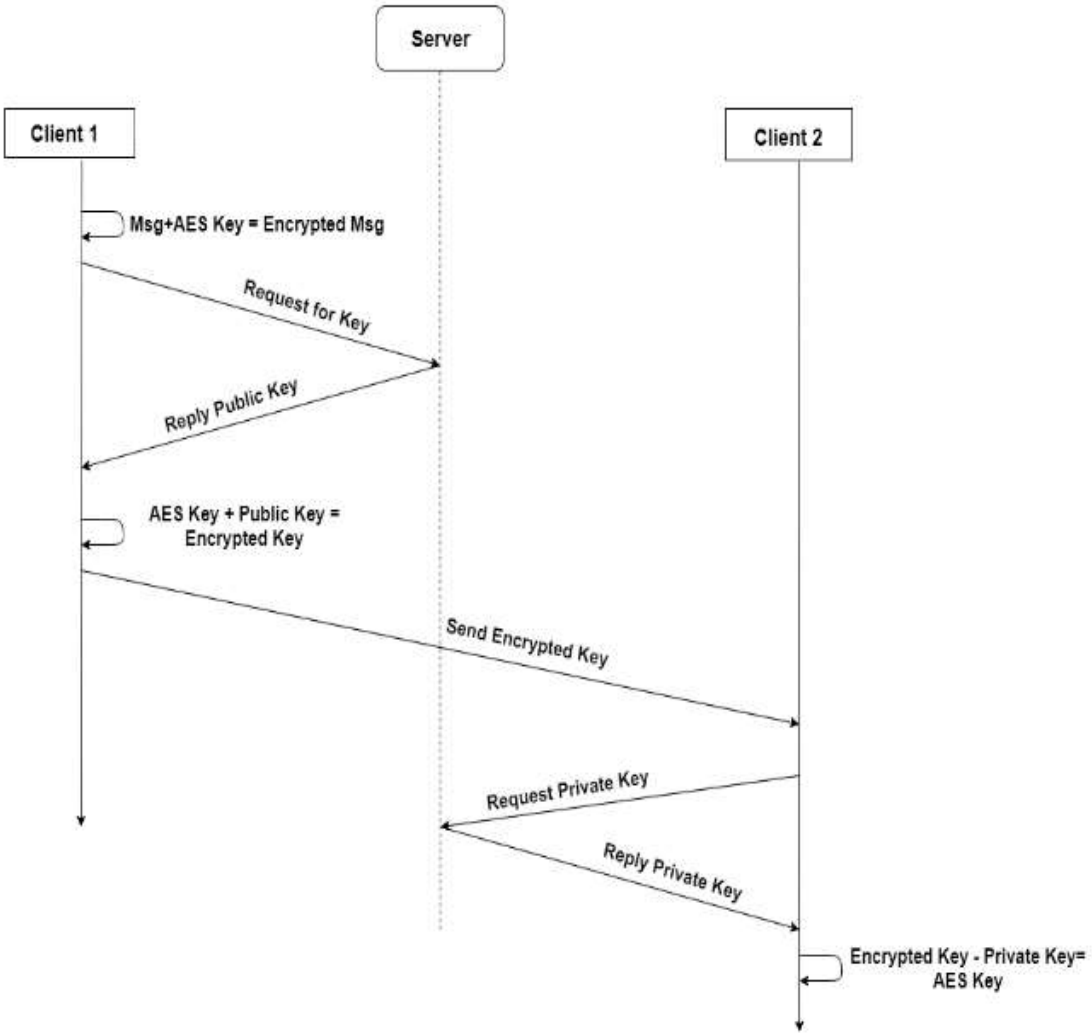


Figure 1: Key exchange protocol

Encoding Process

The data is taken as input from the user of the system, also a secret key is obtained from the user for use in the encryption process. The encryption is then performed using the data and encryption algorithm. After obtaining the encrypted data the cover image is to be selected for the data embedding, then encrypted data is embedded in the image with the help of modified LSB approach. Afterward the encoded image is obtained.

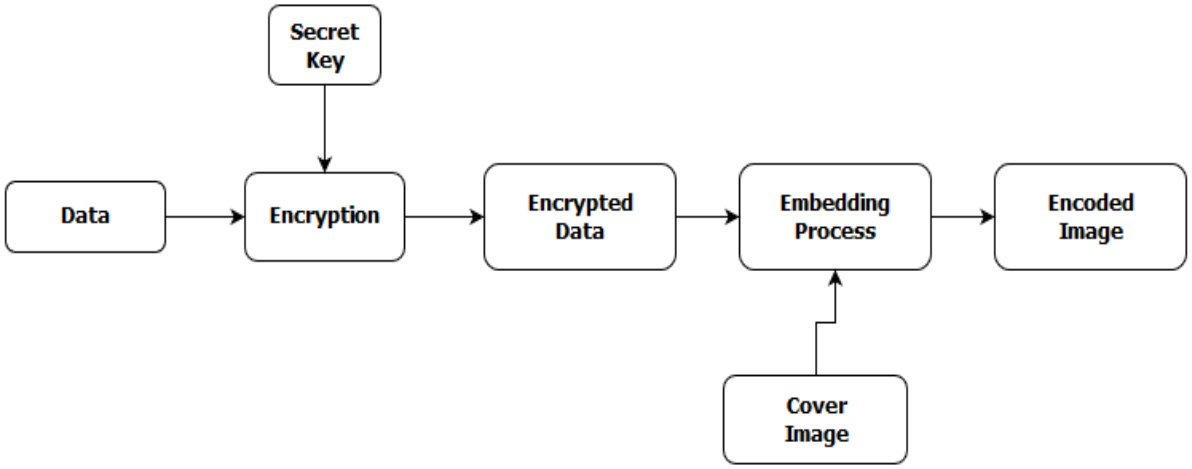


Figure 2: Encoding System Architecture

Decoding Process

The encoded image is taken as input in for the process, decoding is done with modified LSB approach in the same manner as encoding but in reverse order. After decoding the image encrypted data is obtained at the receiver end, the key for decryption is to be obtained for the decryption process. At the end of decryption, the original data is recovered.

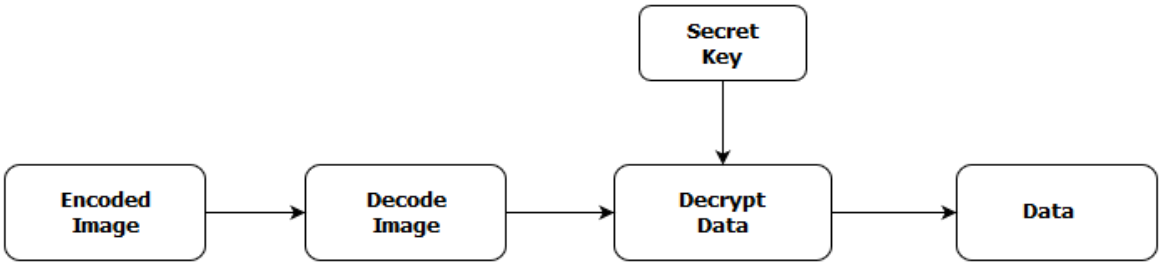
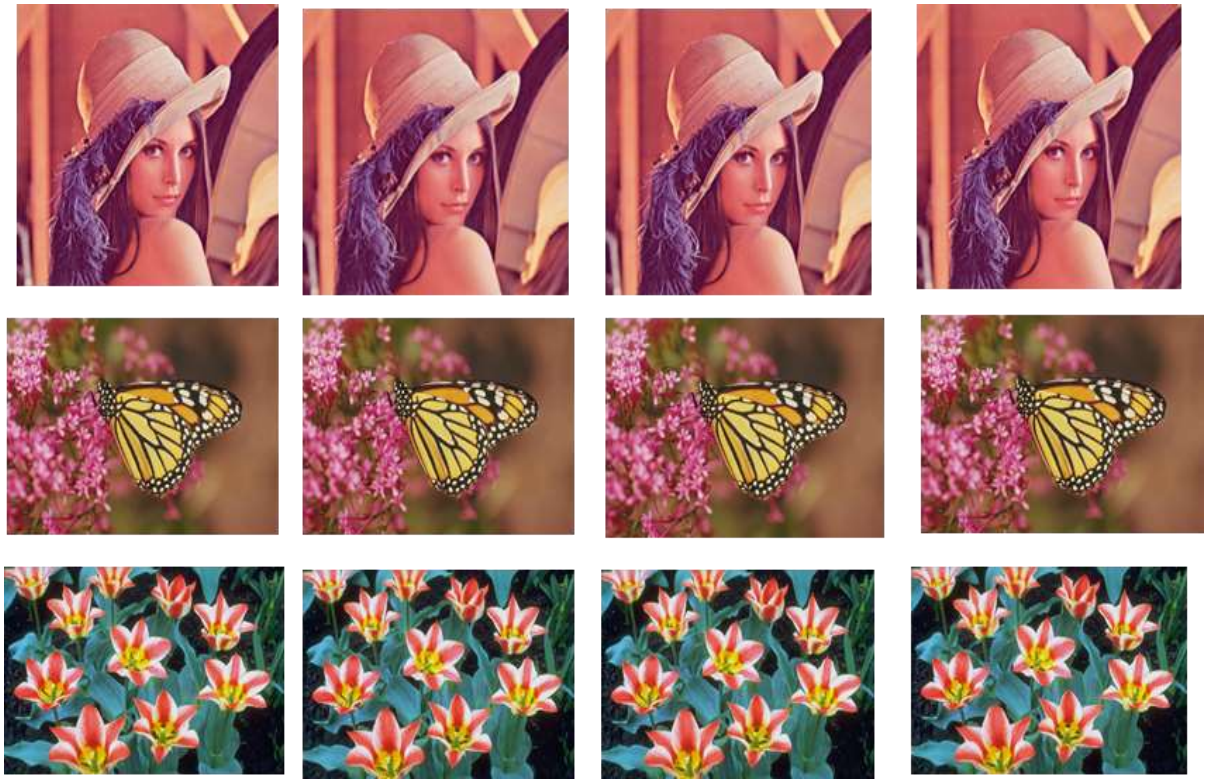


Figure 3: Decoding System Architecture

4. RESULTS

The main objective of the proposed system is to improve the formation quality of the image and increase the security of the data. The cryptography algorithms supplement the security of the data along with the steganography. The AES encryption algorithm is an effective and efficient cryptography procedure. The use of cryptography in the process greatly increases the overall security of the data. The quality of image measured by the MSE and PSNR values is given in Table 1. The higher PSNR values of the image denote that the quality of the image is high.



Original Image **50 characters** **100 characters** **200 characters**

Figure 4: Encoded Images

Table 1: MSE & PSNR Values for Encoded Image

Image name	50 characters (Encrypted characters=108)		100 characters (Encrypted characters=172)		200 characters (Encrypted characters=300)	
	MSE	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**
Lena	0.0108985	67.7571004	0.0175285	65.6933476	0.0306739	63.2631022
Monarch	0.0075124	69.3730105	0.0122197	67.2601814	0.0206527	64.9810203
Tulips	0.0076599	69.2885657	0.0123723	67.2062869	0.0210622	64.8957631

5. CONCLUSION and FUTURE SCOPE

Considering the rapid growth in the digital market, secure communication is set to gain more importance. The consumption of the data over the internet is reaching heights day by day. Work in the field of steganography is going to increase its usability by which the secret communication of potential computer users will also be increased over the internet. The project uses a combination of cryptography and image steganography. Thus the security of data during its transmission has been taken care by converting it into a cipher text using cryptographic algorithm AES and since then it has been embedded into an image with modified LSB algorithm. Higher PSNR values determine the better formation of the encoded image, hence showing the quality perseverance of encoded image. The developed key exchange protocol ensures the secure transmission of the key using asymmetric key cryptography across client for an added level of security.

Further improvements can be done by implementing encryption-decryption in conjunction with other types of steganography. Also, more efforts can be taken into improving the quality of the image which is formed after embedding of the data. Some other algorithms such as DCT which are more suitable for different image formats can be used to implement steganography with fewer calculations.

6. References

[1] Cheddad, J. Condell, K. Curran, & P. Kevitt, (2010). Digital image Steganography- survey and analysis of current methods. Signal Processing, 90, 727-752.

[2] K.B. Raja, C.R. Chowdary, Venugopal K R, L.M. Patnaik, "A Secure Image Steganography using LSB, OCT and Compression Techniques on Raw Images", IEEE International Conference on Intelligent Sensing and Information Processing (ICISP), pp. 170-176, December 2005.

[3] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (IClCT), pp. 749-755, February 2014.

A. Singh and H. Singh, "An Improved Lsb Based Image Steganography Technique For RGB Images", in 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), March 2015, pp. 1-4.

[4] V. L. Reddy, D. A. Subramanyam, and D. P, "Implementation of lsb steganography and its evaluation for various file formats", in International Journal of Advanced Networking and Applications IJANA, 2011, pp. 868-872.

[5] D. Samidha and D. Agrawal, "Random Image Steganography in Spatial Domain", IEEE International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System(EVENT), pp. 1–3, 2013.

[6] S. Chandra, B. Mandal, S. S. Alam, and S. Bhattacharyya, "Content-Based Double Encryption Algorithm Using Symmetric Key Cryptography", Procedia Computer Science International Conference on Recent Trends in Computing(ICRTC), vol. 57, pp. 1228–1234, 2015.

[7] R. M. Samant and S. Agrawal, "Data hiding in gray-scale images using pixel value differencing" in Proceedings of the International Conference; Workshop on Emerging

[8] Trends in Technology, ser. ICWET '11. New York, NY, USA: ACM, 2011, pp. 587-592.

