International Journal of Engineering Research
Volume No.5, Issue No.7, pp : 635-639

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

Encrypted Information Hiding Technique Using BPCS Steganography

Miss. Diptee D. Lad, Prof. Sindhu M.R.
University of Pune, GHRCEM, Pune
laddiptee@gmail.com , sindhu.mrs@gmail.com

Abstract: Data hiding is the very practical problem in today's existence. From previous few month's some researchers work at the records hiding strategies. So, in this paper we're together with some techniques which can already be applied. We are the use of cryptographic and steganographic techniques for hiding the data. Cryptography is the information hiding skill; there is more than one algorithm for cryptography. Here we're introducing AES (Advanced Encryption Standard) algorithm for cryptographic techniques. Steganography hides the facts using one-of-a-kind image wrapper. In this paper we're which includes BPCS (Bit-plane Complexity Segmentation) steganography technique.

Keywords: Encryption, Decryption, BPCS, AES

INTRODUCTION

The requirement of records safety inside an organisation has gone through major modifications within the ultimate several years. The safety of information felt to be precious to business enterprise turned into provided basically through physical and administrative files, earlier than the good sized of records processing equipment. People started doing commercial enterprise on-line and needed to transfer finances electronically, the applications of cryptography for integrity started out to surpass its use for confidentiality. In nowadays global lots of people have interactracted electronically every day by using special manner like e-mails, ATM machines, e-commerce or cell telephones. Information get transmitted electronically, which will give complete confidence about cryptography.

The word 'security' identifies the quality of being secure. To protect the system or data from harm, we have to provide some security. Now a days there are a number of techniques are used for providing security to data. This work provides good security with the help of some techniques like cryptography and stegnography. Cryptography is the type of thing, which is used for transferring plaintext to ciphertext. Numbers of keys are used for providing security. Encryption and decryption are the two methods are used in cryptographic technique. Encryption is nothing but converting data into an unreadable format. Decryption means converting unreadable data into a readable format. Stegnography is the science of hiding information by wrapping message within another message. Stegnography is an effective technique which hides the data and protects the data from unauthorized user. This system uses a combination of two techniques for providing the strongest security on data.

Cryptography is approaching for protective facts in machine structures. This technique writes anonymous code. It consists of the protocols, algorithms and to securely prevent or put off unauthorized access to sensitive information in a conversation. Cryptosystems are not most effective mathematical manner and workstation letters, but additionally it includes the human performance, for deciding on tough-to-flyer passwords, switched off unused structures, and now not spreading sensitive information with outsiders. The method for data encryption and decryption are achieved in two parts Symmetric encryption and Asymmetric encryption [4]. The Symmetric encryption technique uses public key for both encryption and decryption. The one advantage is that there is no need to transfer the key to the sender or receiver side. So, it reduces overburden for key transmission. Another advantage is that the size of the key is same as the size of plaintext. There are a number of techniques for Symmetric Key Cryptography which is having its own advantages and applications. Basically, this paper focuses on Advanced Encryption Standard (AES) [6]. This technique is the strongest technique for hiding the data.

Steganography is the technology of hiding the facts into the alternative data in order that the hidden information seems to be nothing to the human eyes [12]. The phrase steganography comes from the Greek Steganos There are many ways to hide facts interior photograph, audio/video, report and many others. However photograph Steganography has its very own advantages and is most popular among the others. Steganography means actually covered writing. Steganography is the artwork and science of hiding records such that its occurrence can't be detected and a conversation is occurring. A secret record is encoded in a manner such that the very lifestyles of the information is secret. Paired with present declaration methods, steganography may be used to perform hidden exchanges. There are a number of techniques for Steganographic technique. But Bit Plane Complexity Segmentation (BPCS) is the very suitable technique for hiding digital data or image. Cryptographic methods provide security to the content of a message, but Steganography provide hide both the message and the content. So, the proposed system trying to combine advantages of those two techniques for providing security of the data.

RELATED WORK

Image Encryption [1,3,10]

The picture encryption is to transmit the data or image securely over the community in order that no unauthorized consumer can able to decrypt the data or image. Encryption could be described because the conversion of simple message into a form referred to as a cipher text that cannot be read by using any humans without decrypting the encrypted textual content. The message is decrypted by authorized receiver by using a legal decryption key.

$$c(i,j) = E[p_k, m(\bar{i},j), r(i,j)]$$

Where, *E* is the encryption operation.
r(*i*, *j*) is a random value.
Public key of probabilistic cryptosystem *pk* each pixel value *m*(*i*, *j*) where (*i*, *j*) indicates the pixel position [1].

Image Decryption [1,3]

Decryption is the opposite process of encryption that is the process of converting the encrypted textual content into its original undeniable text, so that it may be examined. A licensed user can best decode statistics due to the fact decryption requires a personal or public key. To make the information personal, records is encrypted using a specific cryptographic algorithm. To decrypt the cipher textual content receiver must need to use similar algorithm and then simplest receiver gets authentic records.

$$c(i,j) = g^{m(i,j)} \cdot (r(i,j))^n + \alpha \cdot n^2$$

Where, α is a complexity measure [1].

Data Embedding [3,9]

Records embedding programs can be divided into two agencies relying on the relationship among the embedded message and the cover picture. The first group is formed with the aid of steganographic programs in which the message has no relationship to the cover picture and the cover photograph performs the position of a trick to mask the very presence of communication. The content of the cover image has no cost to the sender or the decoder. In this typical instance of a steganographic software for covert conversation, the receiver has no hobby in the authentic cowl picture before the message become embedded. As a result, there's no want for lossless statistics embedding [7] strategies for such applications.

Least significant bits (LSB) technique [2]

The Least full-size Bit (LSB) is one of the important techniques in spatial domain photo steganography. Like every the steganographic method Least full-size Bit (LSB) wrap a facts into an image. On this approach the least huge bits of some or all byes are changed with a bits of the name of the game message. Image is a collection of number of bits. The blessings of LSB based total statistics hiding approach is that it is easy to embed the bits of the message immediately into the LSB aircraft of image and many strategies use these techniques.

Public Key Cryptography (PKC) [7]

Public Key Cryptography has one challenge is to get the sender and receiver to agree on the key without anyone else finding it. If the sender and receiver are located in different physical location, then they must trust an email or other transmission medium to prevent key. Kay generation, transmission and storage are called key management. Public key is difficult to decode. It is used as a digital signature so sender may always be identified.

EXISTING SYSTEM

Existing System proposed lossless and reversible data hiding [5] techniques. This system used public key cryptographic technique with its probabilistic and homomorphic feature. Lossless scheme uses Least Significant Bit (LSB) plane technique, which replaces the little bits with some new values. This system used LSB technique through Multilayer Paper Coding. After completion of this step replaced bits are extracted from encrypted area, so this operation does not make any effect on authentic plain text image. In the reversible scheme this system introduces preprocessing technique.

Lossless data hiding scheme [1]

Lossless data means data is transmitted without any deficiency. For this scheme existing system introduces PKC technique. Mainly there are three elements one is the image provider. Image provider provides encryption on each pixel [8] of the original image. Second one is data hider, which hides the data using data embedding [9] technique using Multilayer weight paper coding. This technique divides the bit into the block. Receiver understanding the information hiding key additionally exacts the embedded facts.

Reversible data hiding scheme [10,13]

In this scheme preprocessing technique is applied. In this technique image is divided into histogram and then every pixel is encrypted, with homomorphic cryptosystem. This work is done by the image provider. When an image provider applying cryptographic technique then data hider changed the ciphertext value to wrapping a bit which is generated by the additional data. Due to homomorphic property, the encrypted image is minorly changed. If this technique is involved at the decryption side then the image is similar to the original image.

Combined data hiding scheme [1]

Due to lossless technique, data is not affected. There is a minor alteration because of reversible scheme, which directly affects decrypted image. Image is recovered and extract [11] the data are done by receiver. Receiver embed the additional data by lossless technique therefore data can not be extracted after decryption and receiver also adds extra embed data by reversible technique and therefore data can not extracted before decryption.

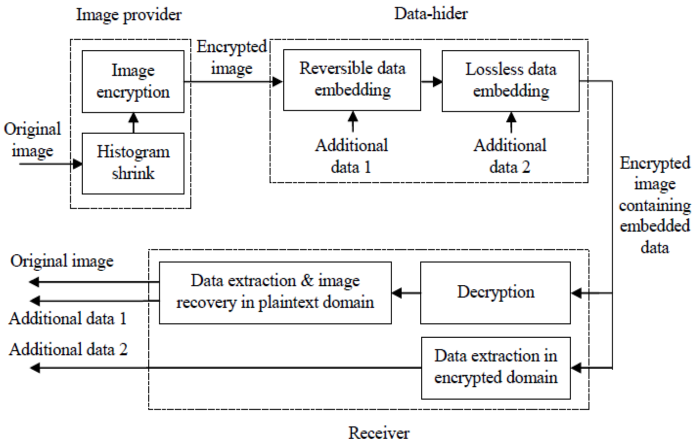

Fig1: Architecture of lossless and reversible data hiding [1]

PROPOSED SYSTEM

We propose a lossless and reversible data hiding using AES and BPCS. The propose system consist of Advanced

Encryption Standard (AES) symmetric key cryptographic algorithm for converting data into an unreadable format. For stegnographic algorithm here we use Bit Plane Complexity Segmentation (BPCS) algorithm. BPCS gives 50-60% accuracy of the result. Another new approach will be added tos the propose system is that it also hides audio data.

Proposed system uses a cryptographic algorithm for encryption and decryption. For proposed system we are using symmetric key cryptography. There are number of algorithm under the symmetric cryptography so, in proposed system we are applying the Advanced Encryption Standard (AES). AES provides replacement of Data Encryption Standard (DES). AES can encrypt data much faster. In AES, all operations are performed on 8 bit bytes. This algorithm is simple to design and it supports variable block length. AES is less expensive than Public key cryptography. It uses fewer bits for encryption.

In the proposed system we are using the BPCS technique for steganography. BPCS technique can hide 50-60% data. It is more beneficial than Least Significant Bit (LSB) because LSB can hide only 10-15% data. So, here we are using BPCS technique. LSB only hides the data with last four bits, but BPCS hides the data using LSB with MSB (Most Significant Bit) planes.

The proposed system is working on text, image and audio also. The sensitive text or the sensitive image or audio is hides using cryptography and steganography technique and deliver it with securely at the receiver side. Audio is also stegno with BPCS algorithm. The main goal of this system is lossless and reversible data hiding and securely provide that data to the receiver side.

Advanced Encryption Standard [6]

The superior Encryption general (AES, also recognized as Rijndael) is famous block-cipher algorithm for portability and affordable protection. The nature of encryption lends itself very properly to the hardware abilities. The superior encryption preferred a 128-bit block cipher, is one of the most famous ciphers inside the global and is broadly used for both business and authorities' functions. Information personal, records is encrypted using a specific cryptographic algorithm. To decrypt the cipher textual content receiver must need to use similar algorithm and then simplest receiver gets authentic records.

Algorithmic Steps:

1. Derive the set of round keys from the cipher key.
2. Initialize the nation array with the block information.
3. Add the initial spherical key to the beginning kingdom array.
4. Carry out 9 rounds of kingdom manipulation.
5. Do the 10th round and for state manipulation.
6. Reproduction the last state array as a encrypted facts.

Bit Plane Complexity Segmentation (BPCS) [13]

Bit plane Complexity Segmentation (BPCS) approach embedding information into bitmap document. The purpose of BPCS is to wrap a fact into a cover picture without detection via human interplay. In BPCS, the vessel image is divided into place first is "informative location" and any other one is "noise-like area", mystery facts is hidden into dummy photo without corruption of photo excellent. In LSB approach last four bits are hidden, however in BPCS technique MSB aircraft with LSB plane provide a security on statistics. The number one aim of BPCS Steganography is to make us of as a lot capability of photograph for information hiding

without a good deal corruption in the visual show of the unique photograph.

Algorithmic Steps:

1. Take one color image for dummy image and finalize size of image.
2. Apply Gray Scale formula for each image.
3. Again finalize the size of Gray Scale image.
4. Convert dummy and secret image in PBC and CGC form.
5. Apply Bit Plane Slicing on dummy and secret image.
6 . Calculate 'alpha' (α)
7. Perform conjugation and embedding technique one after another.
8. Convert CGC to PBC image.

Architecture of Proposed System:

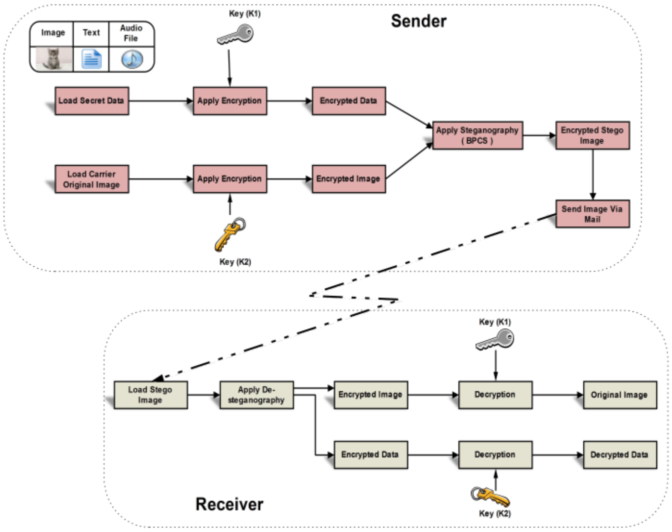

Fig2: Architecture of proposed system

1. Load Secret Data:-

Load the data which is in the form of image, text or audio file. This is the input for the application.

1. Apply Encryption:-

This is the cryptographic step. So, in proposed system AES algorithm is used for encryption.

2. Encrypted data:-

After applying AES technique with encryption algorithm we will get encrypted data.

3. Load carrier original image:-

Load another image for , it work as a wrapper image. This image helps to embed the data in BPCS technique.

4. Apply Encryption:-

For providing two layer security, provides encryption on wrapper image.

5. Encrypted image:-

After performing encryption on wrapper image we will get encrypted image.

6. Apply Stegnography:-

   For stegnographic technique we are using BPCS algorithm.

7. Encrypted Stego Image:-

   So, we will get the combination of AES and BPCS technique which is in form of encrypted stego image.

8. Send image via email:-

   Send the encrypted stego image to the receiver via email.

   Perform same Procedure at the receiver side for decryption. For decryption purpose same key will be used. If the original senders data and the receiver received data is same then only we can say that the data is lossless.

RESULT ANALYSIS

PSNR is Peak Signal to Noise Ratio. It describes the quality between original image and compress image. If the value of PSNR is high, then the quality of compressed image is better. PSNR is measured in decibels i.e. dB. In PSNR square of the peak value in image is taken and it divided into Mean Square Error. If the PSNR is good that means ratio of signal to noise is higher.

PSNR is defined via Mean Squared Error (MSE).

Noise-free m×n monochrome image I and its noise

Approximation K, MSE is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)^2$$

$$PSNR = 10.\log_{10}\frac{MAX_I^2}{MSE}$$

PSNR is defined as:

$$= 20.\log_{10}(\frac{MAX_1}{MSE})$$

$$= 20.\log_{10}(MAX_I) - 10.\log_{10}(MSE)$$

Image	**PSNR Table**		
	Message Size	***Data size***	***PSNR***
Image 1	500×500	10 KB	0.329
Image 2	500×500	20 KB	0.429
Image 3	500×500	40 KB	0.567
Image 4	500×500	70 KB	0.678

Fig. 3: Original image

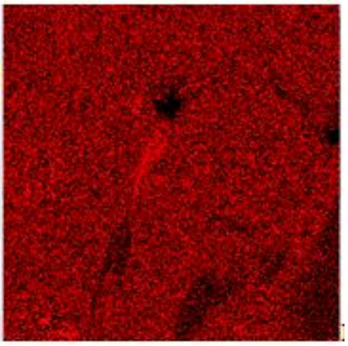

Fig. 4: Bit plane separation of Original image

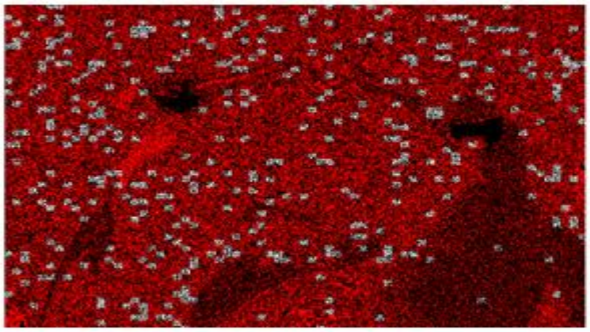

Fig. 5: Analysis current Bit plane with α-0.55

Future Scope

If the PSNR is good, that means the ratio of signal to noise is higher. With a good PSNR ratio we can achieve less loss of data. So, in future we are trying to improve PSNR.

Conclusion

In the government sector, there are some confidential documents so, we need to provide security to these documents while document transmission. The Military requires strong security for blueprints transmission. So, "Encrypted Data Transmission using BPCS algorithm" helps to achieve the required level of security with less data loss. Lossless data hiding in encrypted images is a new topic, drawing attention because of the privacy-preserving requirements of data management. A Previous method implemented an LSB technique, which embed the data with vessel data for security purpose. This system uses BPCS technique for providing more security on data. It can encrypt text, image or audio into image. For that purpose this system provides AES algorithm for encryption. So, from this technique we will provide more security on our data.

Acknowledgment

I take this opportunity to thank Prof. Sindhu M.R. for her valuable guidance and for providing all the necessary facilities and her suggestions.

References

i. Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography," IEEE Transactions on Circuits and Systems for Video Technology 2015

ii. Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012 International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 4.

iii. Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image," IIEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011.

iv. Mehran Mozaffari-Kermani, Arash Reyhani-Masoleh, "Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard," IEEE TRANSACTIONS ON COMPUTERS, VOL. 59, NO. 5, MAY 2010

v. B.Elang kavin, Dr.B.Latha, "Reversible Data Hiding In Image Encryption With Efficient Compression And

Enhanced Security," ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.

vi. *Alan Kaminsky, Michael Kurdziel Stanisław Radziszowski, "An Overview of Cryptanalysis Research for the Advanced Encryption Standard," The 2010 Military Communications Conference - Unclassified Program - Cyber Security and Network Management 2010 IEEE*

vii. *Mr. Madhusudhan Mishra, Mr. Gangadhar Tiwari, Mr.Arun Kumar Yadav, "Secret Communication using Public key Steganography IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014),May 09-11,2014, Jaipur, India*

viii. *Masoud Nosrati Ronak Karimi Mehdi Hariri, "Reversible Data Hiding:Principles, Techniques, and Recent Studies," Masoud Nosrati et al., World Applied Programming, Vol (2), No (5), May 2012*

ix. *Mehdi Hussain, M. Hussain, "Embedding Data in Edge Boundaries with High PSNR," 978-1-4577-0768-1/11/$26.00 ©2011 IEEE*

x. *Arun K Mohan, Saranya M R, K. Anusudha, "An Algorithm for Enhanced Image Security with Reversible Data Hiding," 978-1-4799-6629-5/14/$31.00_c 2014 IEEE*

xi. *Shruti M. Rakhunde, Archana A. Nikose, "A Novel and Improved technique for Reversible Data Hiding using Visual Cryptography," international Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014*

xii. *SHRIKANT S. KHAIRE, Dr. SANJAY NALBALWAR, "Review: Stegnography- Bit Plane Complexity Segmentation, " International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4860-4868*

xiii. *Ms. Nuzhat Ansari, Prof. Rahila Sheikh, "Reversible Data Hiding in Encrypted Image: A Review," @IJMTER-2014, All rights Reserved*