International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2015): 3.791

A Review Paper on Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption

Malhar Bhambure[1], Karan Bhalgat[2], Mayur Rathod[3], Shalaka Deore[4]

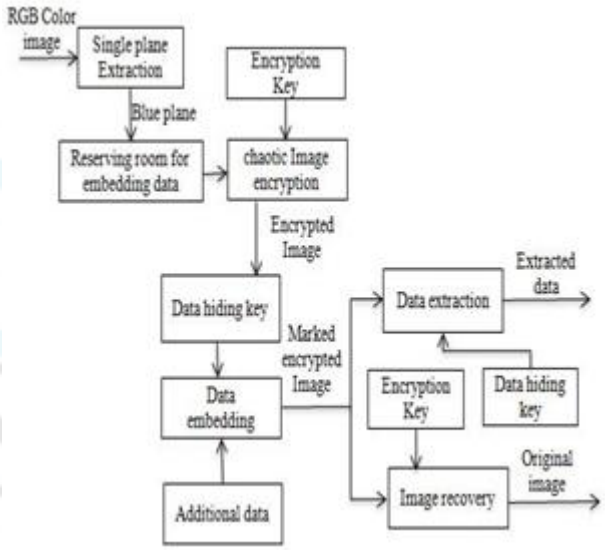
[1]Modern Education Society's College of Engineering, Pune, Savitribai Phule Pune University
[2]School of Computer Science and Engineering, Chung-Ang University, 221, Heukseok-dong, Dongjak-gu, Seoul 156-756, Korea
[3]Monash University, Department of Management, McMahons Road, Frankston 3199, Austria

Abstract: ***In digital era, lots of data is generated over web and in local data exchange mediums. Private companies, government organizations, internet users, etc. are prime source of data generators over globe. As loads of data is generated every day, security and integrity of data becomes the most important factor. Confidentiality of data is prime key of concern of every organization working in digital world. In this paper, we introduce a novel technique in which data is encrypted in images and then transmitted to client (user). In this paper, for hiding data in encrypted images we use Reversible Data Hiding (RDH) using reserving rooms in advance approach. By using this approach we can recover image without any loss of data. Previous system use to vacant room before encryption which may result in some errors or attacks by intruders which causes defect in confidentiality of data. In our proposed system, image recovery and data extraction are free from any errors and attain real reversibility. In this paper, AES encryption algorithms, visual cryptography algorithm for colored images, LSB based steganography, algorithms are implemented on various data patterns. The algorithms are compared and evaluated on accuracy and its ability to reproduce original data.***

Keywords: Reversible Data Hiding, Encryption, Data extraction, Steganography, Cryptography

1. Introduction

In the recent years a lot of attention is being paid to reversibly hide data in encrypted images, since it maintains a very great property of lossless recovery of the original image cover soon after the embedded data is extracted while protecting the image's confidentiality. All the previous methods did was embed data by reversibly vacating the room for encrypted images, thus making it vulnerable to few errors on data extraction and restoration. In this method we propose a great and an highly innovative method of reserving the room before the encryption of images using AES(Algorithm Encryption Standard) along with traditional RDH(Reversible Data Hiding), making it easy for data hider to hide data by embedding the data in encrypted images. The respective proposed method thus achieves great reversibility that is data extraction and image recovery are free from errors and a secure transfer of data which is flawless.



2. Previous Works

Wei Liu et al provides scheme for compressing image progressively by resolution. It incorporates of a decoder which can observe low resolution of image and study its variation statistics. These statistics are used decode next levels of resolution. The task of encoder is to send down sampled version of cipher text. The decoder does two tasks i.e. it decodes and decrypt images. This process is continued until whole image is decoded.

Problem with algorithms was that all blocks are encrypted in homogeneous manner. Second problem is that, block encryption is not robust and third problem faced is data integrity. The combination of data hiding and encryption in reversible manner as proposed by W. Puech el at. Solves the problem. A new frame work was proposed by Christophe Guyeux el at, in which he developed framework for information hiding called chaos-security which claims to deepen security levels in information hiding. Our proposed system is combination of various algorithms which gives rise to a much better framework for secured transmission of data.

3. Encryption Algorithms

Encryption is the process of converting a plaintext message into cipher text which can be decoded back into the original message. An encryption algorithm along with a key is used in

the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers. The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message.

3.1 AES Algorithm

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plain text using the same encryption key.

3.2 Visual Cryptography Algorithm for Encrypted Images

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

Step 1:

a. In 1st step we convert RGB value of each image into CMYK form. To achieve this we form three share images.

b. Share1 will contain pixels with only C value as 1 and other values 0. Share2 will contain pixels with only M value as 1 and other values 0. Share3 will contain pixels with only K value as 1 and other values 0.

Step 2:

a. In this step for each share image we will take 1 cover image.
b. Then share1 is added to cover1 by dividing pixel value by 5(e.g. divide C by 5)

Same process is repeated for all share images.

3.3 Least Significant Bit Steganography

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are

sufficient to hold one message byte. Rest of the bits in pixels remains the same.

4. Data Hiding and Image Encryption

The process of data hiding and image encryption in this method is carried out in four steps. But before the process begins. The sender logs into the application using a valid user id and a password. This GUI is provided to ensure a higher degree of security even before the actual process begins. Thus with such high secureness there lies a very small line for an intruder to sniff into the transfer. The process of actual data hiding and encrypting the images along with embedding them with data is as follows. In the first step the image selected by sender is divided into three shades. These shades are decomposed in such a way that we get decomposed image components as Red, Green and Blue. These decomposed images form RGB plane for each of the components, thus resulting in the first plane being the red plane, the second to the green plane and the third to the blue plane. So the conclusion is that a color image is formed by stacking the three planes together, like a sandwich. The second step is reserving room before encryption for the data. The first stage can be divided into two steps: the image partitioning and self-reversible embedding. Initially, image partition step divides blue plane of the original image chosen by the sender, into two parts say A and B; then, the LSBs of A are reversibly embedded into B with a standard RDH algorithm using interpolation so that LSBs of A can be used for accommodating messages. Now finally the final stage is known as image encryption. Here in this stage we use Algorithm Encryption Standard (AES Algorithm) to encrypt the image for secure transfer over the network. It encrypts the original image pixel values with encryption key value. We use public key encryption method to generate the keys. The final stage is hiding the data in encrypted images. Hence after having the idea of how many bit-planes and the rows of the pixels data hider or sender can modify, the data hider thus simply uses a side-match prediction method or simply a LSB replacement approach to swap the available bit-planes with additional data that he intends to send securely without making it vulnerable to threats. In side-match prediction approach the histogram is created by exploiting the difference in all the values between pixels and their predictive values. All predictive error values are transformed into histograms to create higher peak values. In the extraction and reversing process, the side-match prediction is applied to the stego-image, and the created histogram is processed for extraction and reversing. Finally, the data hider sets a label following 'n' to point out the end position of embedding process and further encrypts 'n' according to the data hiding key to formulate marked encrypted image.

5. Data Extraction and Recovery

The data extraction and recovery is a complete reverse of the previously discussed hiding and encryption. The receiver initially logs in with his valid user id and a password. Then he finds the Encrypted image with the data hidden into it. The process that takes place is as follows. With the encryption key only, an approximate image can be reconstructed with high quality. The receiver is expected to have its corresponding encryption key. Receiver sides are provided: with the encryption key only, with the embedding key only, and with both the encryption and embedding keys. There is yet another special situation in which the receiver obtains the encryption key first and unexpectedly receives the embedding key much later. In the previous methods, when the receiver acquires the embedding key later, he/she still cannot extract the hidden message from the decrypted image directly, unless the marked encrypted version has been saved (this is likely the case) and is used, or extra re-encryption is carried out using the encryption key to regenerate a marked encrypted copy. In this proposed method, the receiver can save the LSB bits of the marked encrypted image before estimating the original image. After the embedding key later is acquired later, the receiver can extract the additional bits from the save bits.

6. Motivation

The motivation of the proposed method comes from a wide range of work and business environments. One of them being secure transfer of student data from a college to its respective affiliated university. Here when a college is supposed to send data about their bonafides, the university official sends it using simply an email. As we know emails are subject to many threats and easily accessible by intruders, it may result into manipulation of records resulting into catastrophic consequences to both parties. By making use of proposed method, the transfer of data becomes significantly secure thus eliminating its vulnerability to threats and intrusion. This thus became a primary reason and a motivation to develop such a secure system for the betterment and improvement of operations for big corporations. The proposed method can also be used in many fields which include banking, production, investigation, international protocols transfers and many more.

7. Conclusion

Reversible data hiding in encrypted images has become of the finest and the most secure way of transferring data. It becomes almost impossible for an intruder to even notice presence of valuable and critical data in an image if by any chance he manages to obtain it. Also providing a login functionality to the application thus provides a higher degree of security to it making the operation and the application limited. In this method we propose a significant method of using a combination of algorithms and methods for providing a fine high quality final product. The data hiding and image encryption accounts to use of combination of methods. The process is carried out by using AES Algorithm, Visual Cryptography for Encrypted Images along with LSB Steganography. The data extraction and recovery is equally secure as the encryption method. Unless and until the receiver has a valid user id, password and the respective keys, he stands no chance generating the data. Finally after generation of data at the receiver side is completed. The process is said to have been a success.

References

[1] Besteena K, Philumon Joseph, "Reversible Data Hiding in Selectively Encrypted RGB Images by Reserving Room in Advance", 2014 First International Conference

on Computational Systems and Communications (ICCSC) | 17-18 December 2014 | Trivandrum
[2] Zhenxing Qian, Xinpeng Zhang, "Reversible Data Hiding in Selectively Encrypted RGB Images by Reserving Room in Advance", IEEE 2014.
[3] Xiaolong Li, Bin Yang, and Tieyong Zeng," Efficient Reversible Watermarking Based on Adaptive Prediction
[4] Error Expansion and Pixel Selection", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 12, DECEMBER 2011
[5] Weiming Zhang, Biao Chen, and Nenghai Yu, "Improving Various Reversible Data Hiding Schemes Via Optimal Codes for Binary Covers", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 6, JUNE 2012.
[6] Guided by Prof. Shalaka Deore (Internal Professor), Modern Education Society's College of Engineering, Pune, Savitribai Phule Pune University