A New Hybrid Approach CryptsteG of Data Hiding in Images Using Cryptography and Steganography

Pria Bharti, Roopali Soni
M. Tech. Scholar, Assistant Professor
Department of CSE, OCT, Bhopal, India

Abstract-Cryptography is the science of using mathematics to encrypt and decrypt data and Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. A novel scheme for the embedding data in images is CryptsteG in this method we combined cryptography and Steganography process in one algorithm. First we encrypt the data and then embed with image with new Steganography algorithm. The method is very efficient especially when applied to those images whose pixels are scattered homogeneously and for small data. The given image is partitioned into four level blocks, and the data will be embedded into selected the four diagonal sub-blocks values depend upon key. This algorithm only requires fewer steps and it can embed data efficiently without discarding image. Embedding 4 bits information in a 4*4 pixel block need to change very less pixels on average. Furthermore, the quality of the produced stego-images is better than that of other methods. The quality of stego-image is greatly improved when our algorithm is used.

Keywords: Cryptography, Steganography, Security, Data, Hiding, Quality, Image.

I. INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication [1]. The Steganography hides the message so it cannot be seen; Cryptography scrambles a message so it cannot be understood [2]. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for improved concealment and security. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In fact, steganography can be useful when the use of cryptography is forbidden: where cryptography and strong encryption are outlawed, steganography can circumvent such policies to pass message covertly. However, steganography and cryptography differ in the way they are evaluated: steganography fails when the “enemy” is able to access the content of the cipher message, while cryptography fails when the “enemy” detects that there is a secret message present in the steganographic medium. The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis [3]. The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages. The aim of this paper is to describe a method for integrating together cryptography and steganography through some media such as image, audio, video, etc. In this paper, we propose a new algorithm for color full image. According to the method, a given image is partitioned into 4*4 blocks, and then take only diagonally block for data hiding. Various data hiding techniques, for instance, LSB (Least Significant Bit) approach, have been developed in recent years, most of them are for color and gray scale images and our method is also for color images. Although Steganography is applicable to all data objects that contain redundancy, in this article, we consider BMP images only (although the techniques and methods for steganography and steganalysis that we present here apply to other data formats as well). People often transmit digital pictures over email and other Internet communication, and BMP is one of the most common formats for images. Moreover, steganographic systems for the BMP format seem more interesting because the systems operate in a transform space and are not affected by visual attacks.[4] (Visual attacks mean that you can see steganographic messages on the low bit planes of an image because they overwrite visual structures; this usually happens in BMP images.) Neil F. Johnson and Sushil Jajodia, for example, showed that steganographic systems for palette-based images leave easily detected distortions.[5] The rest of this paper is organized as follows: A detailed review on related research is discussed in section 2. The proposed method is presented in section 3. Experimental analysis and discussion is given in section 4. Finally, conclusion will be presented in section 5.

II. RELATED RESEARCH

The “uneven embeddability” problem has been addressed in [11] earlier, in which a random shuffling key is used to shuffle the image so that the “flippable” pixels are distributed uniformly throughout the image. In this paper, we handle the “uneven embeddability” of the image by embedding the watermark adaptively in those “embeddable” blocks. In [10], the original image is partitioned into 3*3 blocks. In a block, flipping priorities are computed, and then modifying the total number of black pixels to be either odd or even embeds data bits. The
flipping priorities are determined by considering smoothness and connectivity which are connected to human perception. The smoothness is measured by horizontal, vertical, diagonal and anti-diagonal transitions (from “1” to “0” or the vice versa for two pixels that touch each other) in a 3*3 window, and connectivity is measured by the number of the black and white clusters. Some images require a shuffling key in order to distribute the “flippable” pixels all over the image. The randomness in choosing the embedding locations creates poor visual effects despite the large capacity. Further improvements on visual quality is made by choosing the edge pixels in our paper that is the problem in [11], the proposed scheme uses a secret key and a weight matrix to protect the hidden data, it also uses a weight matrix to increase the data hiding ratio. The operator XOR is adopted so that the keys can not be compromised easily. The original image is partitioned into blocks of size m*n. In each m*n block Fi, b1, b2,…,br is the r bits of data which will be embedded into the block by the invariant I1.

\[ I1: d = b_1b_2…b_r - \sum [F_i \oplus K] \odot W \mod 2^r \]

In invariant I1, let \( \oplus \) be the bitwise exclusive-OR, \( \odot \) be the pair-wise multiplication operator on two equal size integer matrices. The embedded data will be extracted by the invariant I2.

\[ I2: b_1 b_2...b_r = \sum [F_i \oplus K] \odot W \mod 2^r \]

Given an m*n host image, the scheme can hide as many as \( \log_2 (mn+1) \) bits of data in the image. However the connectivity issue has not been taken into consideration during the embedding process. In [4], Pan et al. proposed a novel data hiding method by partitioning an image into blocks, where each block was partitioned into overlapping sub-blocks. Each sub-block is connected with a level number according to its pattern, indicating influence on visibility by assumed change of the central pixel in the sub-block. Data will be hidden by changing the central pixel in a sub-block. In [5], the LSB is the most popular Steganography technique. It hides the secret message in the RGB image based on it its binary coding.

Figure 1 presents an example about pixel values and shows the secret message. LSB algorithm is used to hide the secret messages by using algorithm 1. LSB makes the changes in the image resolution quite clear as well as it is easy to attack[16].

III. THE PROPOSED METHOD

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 2. In BMP image (e.g. scanned image) there are 3 color data values for one pixel, that is, red, green and blue.

![Block Diagram of Algorithm](image-url)

**Fig.2 Block Diagram of Algorithm**

To save storage, there is 24 bit representation for each pixel. So hiding without significant distortions is very difficult for BMP images. We have mentioned that arbitrarily flipping a pixel in a BMP image could be easily...
noticed. So only pixels on the boundary may be modified, and it also needs some constraints. Based on this criterion, we propose a new method in this paper. The new method consists of two parts: embedding and extraction process. The entire process of embedding and extraction is illustrated in Fig. 2.

A Embedding process
The embedding process involves partitioning the original image into blocks, calculating characteristic values from the blocks and hiding data process. More details will be discussed in the following subsections.

1 Encryption (Secret Text to Encrypted Text)
Input: Secret Text and Secret Key
Output: Encrypted Text
Algorithm:
Step 1: Concat Key 8 Times and then Choose first eight characters from KEY as (c1,c2,c3,c4,c5,c6,c7,c8)
Step 2: Convert each character (o/p of Step1) into ASCII and sum and divide from 1000 and reminder of this process is our Final Key of three digit number (N1,N2,N3)
Step 3: according to these three numbers (N1, N2, N3) we change our original message into cipher message we use shift encryption and every 1,4,7,….. character shift by N1
every 2,5,8,…..character shift by N2
every 3,6,9,…..character shift by N3 and we get cipher text

2 Steganography
Suppose we have an image P which dimension is exactly divided by 4 and we partitioned image into 4*4 sized blocks. Partitioned block Fig 3(a) illustrates the partitioned block diagram for the original image P.

Steganography Algorithm (image To Stego Image)
Input: Secret Text, Secret Key, Image
Output: Stego Image
Algorithm:
Step 1: For Placing Data into images pixel first we will calculate DataPositionArray by concating of ASCII of N1, N2 and N3.
Step 2: Choose first 20 characters from DataPositionArray which is 24 characters long
Step 3: Count 1 in this 20 character long DataPositionArray
Step 4: Calculate size of Cipher Text ( StrLEn) in Bites Strlen=String Length(ciphertext) * 8
Step 5: Now SizeOfImage (Length X Height ) should be greater than Show The Minimum Image Size ( Length X Height ) as that [(CountOne/20)*(1/4)*(Length*Height)] > StrLen Convert cipher text into array of bits and then make 4 X 4 pixel Block and choose block according to DataPositionArray
Step 6: Convert LSB Bit of block Diagonal pixel After inserting all cipher text bit we get final image

B Extraction Algorithm
Input: Stego Image, Secret Key
Output: Plain Text
Algorithm:
Step 1: Receiving the stegoimage P.
Step 2: Convert image into 4X4 pixel Block as like of embedding algorithm.
Step 3: Choose Diagonal pixel according to data position-array and collect the LSB of diagonal pixel from selected block and make Cipher Text.
Step 4: This Cipher Text is input for decryption algorithm which is reverse of encryption algorithm and get plain text.

IV. EXPERIMENTAL RESULTS
The algorithm is code in Matlab and run on a Windows 7 platform. The method is applied to several BMP images. In our experiments, we use 32 Bytes English text document and 512X512 ‘lenna’ images. Figure 3.1 illustrates a 512X512 original image and we can hide 256 bits in the original image which is shown in Figure 3.1 The stego-image is shown in Figure 3.2 are embedded in it using the proposed techniques. The pixels in ‘lenna’ image are very approximately uniformly distributed; therefore, we have difficulty trying to detect the hidden data by naked eyes.

Fig 4 Original Image
Fig 5 Stego Image
We have successfully applied our proposed algorithm to commonly used color images such as Lena, Baboon and Boat color test images; only one color plane is applied by the algorithm.
Table I. Test Results for 512 x 512 x 24 Color Images

<table>
<thead>
<tr>
<th>Image</th>
<th>PSNR(dB)</th>
<th>Capacity (bits)</th>
<th>Robustness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>36.3</td>
<td>812</td>
<td>7</td>
</tr>
<tr>
<td>Baboon</td>
<td>35.1</td>
<td>598</td>
<td>1.4</td>
</tr>
<tr>
<td>Boat</td>
<td>36.7</td>
<td>578</td>
<td>9</td>
</tr>
</tbody>
</table>

Note that there is no noise in all of tests since the proposed algorithm does not use modulo-256 addition. The embedding capacity can range from 512 to 1024 bits for the purpose of authentication, and it can be adjusted by changing the block size for other applications. As shown later the PSNR is much higher than that obtained by using the method in [17]. It is noted that the data embedding capacity and the PSNR of the marked image versus the original image can be adjusted according to the password (key). Since these two performance parameters are usually conflicting each other in the sense that if the embedding capacity is improved, the PSNR will drop and vice versa, there is usually a tradeoff between the data embedding capacity and the PSNR of the marked image versus the original image for a targeted application.

V. CONCLUSION

In this paper we propose a new method to embed data in BMP images. This method shows its larger capacity for hiding data than other methods without loss of imperceptibility. 4 bits data can be embedded in a 4x4 block and some blue part of pixels need to be changed on average. Experimental results show that the method is very efficient especially when applied to those binary images whose color pixels are distributed nearly uniformly.

REFERENCES


AUTHOR’S PROFILE

Pria Bharti received B.E. degree from BITs, RGPV in Computer Science and Engineering. She is currently pursuing M.Tech in computer Science & Engg. in Oriental College of Technology, Bhopal. Her research interests include image processing and network security. She is published 1 international research paper.

Roopali Soni received M.Tech degree from SOIT, RGPV in Computer Technology and Application. She is currently Head of computer Science & Engg. Department in Oriental College of Technology, Bhopal. Her research interests include soft computing Data Mining and warehousing and Object Oriented Concepts.
Ms. Soni is a life member of ISTE & Institutional Member of CSI. She is published 15 international and 12 national research papers. She was awarded (best paper) for the paper entitled as “The Role of Industry Institute Interaction for Technical Institutions” in the national seminar on “Teaching Methodology in Present Global Teaching Education” sponsored by ISTE.