A Secure and Robust Method for Image Steganography by AES Method of Encryption.

Nikita Mhase 1, Dr. Kalyani Akant 2

1Department of Electronics and Telecommunication, G.H. Raisoni College of Engineering, Nagpur-16, MH.(INDIA)
2Associate Professor, Department of Electronics and Telecommunication, G.H. Raisoni College of Engineering, Nagpur-16, MH.(INDIA)

Abstract - The speedy development in exchange of data through digital media made it easy to exchange the data to the destination quickly. There are large number of transmission mediums to transfer the data to destination like e-mails; simultaneously it may be easier to change and misuse the valuable information through tampering and hacking. So, in order to transfer the data securely to the destination without any alteration, there are many approaches like Cryptography and Steganography. This paper deals with the secure transfer of audio signals to the destination. This is achieved by encrypting the image with a secret message and then using the AES algorithm to perform steganography. The outstanding progress of digital technology has increased the ease with which digital data is reproduced and retransmitted. However, since the advantages of such a progress are broadly available, they give equally increasing potential to both legal and unauthorized data manipulation. Consequently, the necessity for the copyright protection of digital products against unauthorized recording attempts is known as data piracy.

Keywords: AES, Caesar-cipher, DWT, Encryption, Secret key, Steganography.

I. Introduction

Steganography is the art of writing the hidden messages in such a way that no one else, other than the intended receiver knows the existence of the secret message. The word “steganography” is obtained from Greek words, meaning “hidden/secret writing”. The word is divided into two parts: steganos which means “secret” and “graphic” which means “writing”. However, in hiding information, the meaning of steganography is hiding secret messages or text into some other media file such as text, image, sound or video. The word “steganography” is often considered similar with “cryptography” and “watermarking”. Watermarking ensures message integrity, cryptography scrambles the message, and steganography hides it. In digital steganography, digital communications may include steganographic coding of a transport layer, such as a document file, image protocol, file, or program. Media files are ideal for steganographic transmission because of their large size. For example, a sender starts with a pure image file and adjusts the image colour of every 100th pixel of the image which corresponds to a letter in the alphabets; a change is so precise that someone not specifically looking for it is unlikely to notice it.

This paper is based on the idea of sending an audio signal secretly by hiding it in an image which is used in the applications like Defence, Air force, Air traffic control, etc. The need arises to keep your actions secret from your opponent.

II. Related Work

The research concerned here is to hide the audio in the image so smoothly such that it is inaudible to the listener. The method used to hide the audio signal is very simple. Initially the audio signal is watermarked using an Image (1). The technique used for watermarking of audio signal is Discrete Wavelet transform (DWT). Then a secret message is asked as an input to the user. The work uses Caesar cipher method to change the secret message (original key) (key1) to a new
keyword (key2). The new key (key2) thus formed will be actually hidden in the image (2) rather than directly hiding the original key (key1) given by the user. To this encrypted Image (2) the watermarked audio signal with Image (1) is Steganographed. This steganography is done by Advanced Encryption Standard (AES). The invention includes three major processes:

1) Audio Watermarking
2) Hiding Secret code in an image
3) Steganography of watermarked Audio signal in encrypted Image (AES algorithm)

**1) Audio Watermarking:**
An audio watermark is a unique electronic mark embedded in an audio signal. The embedding procedure performs three major operations; pre-processing of watermark, frequency decomposition of the audio signal based on DWT, and embedding of watermark in the DWT-transformed audio signal. The details are described in the following steps.

1. Express the grey-scale image1 watermark as a two-dimensional matrix whose size is X1 x X2.
   \[ \text{Image1} = \{ \text{Image1}(i,j), 1 \leq i \leq X1, 1 \leq j \leq X2 \} \]
2. Convert the two-dimensional image1 matrix in one-dimensional column vector V of length \[(X1 \times X2):1\].
3. Normalize the one-dimensional vector V by dividing each element by 255. Then vector is denoted by Vn.
4. Apply a two-level DWT to the audio signal. The DWT operation produces the one-dimensional sub-bands shown in Fig 1, where A2 is the approximation coefficient, and D1 and D2 are the first-level and second-level detailed coefficient, respectively. It’s important to note that the decision to adopt the DWT was the fact that it gave better results than the other watermarking techniques as shown in table.1.

**Fig. 1: Decomposition of DWT.**

<table>
<thead>
<tr>
<th></th>
<th>CA Modification</th>
<th>CD Modification</th>
<th>LSB Slicing (1 Image)</th>
<th>Slicing (2 Images)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>64.766</td>
<td>64.49</td>
<td>69.2997</td>
<td>69.4291</td>
</tr>
<tr>
<td>SNR</td>
<td>48.468</td>
<td>48.21</td>
<td>44.0180</td>
<td>44.7790</td>
</tr>
<tr>
<td>Robustness</td>
<td>0.9230</td>
<td>0.9230</td>
<td>0.4513</td>
<td>0.9956</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.6990 (Image 2)</td>
</tr>
</tbody>
</table>

5) Embed the normalized watermarked vector Vn, into the second-level detailed Coefficient D2 by X-ORing each elements of the vector Vn with the coefficient D2. The embedding procedure produces the watermarked second-level detailed Coefficient (VD2).

**2) Hiding Secret code in an Image:**
The secret message (key1) is taken as an input from the sender. The Secret code acts as a password while decrypting audio signal. The secret code is transformed by Caesar Cipher method to a new code key (2) before hiding.

a) Formation of secret Key(key2) Using Caesar Cipher Method

The Caesar cipher is a substitution cipher in which each letter is 'shifted' a certain number of places next to the alphabet.
The action of a Caesar cipher is to replace each text letter with a different one by a fixed number of places next to the alphabet. The cipher illustrated here uses a right shift of three, so that (for example) each occurrence of B in the plaintext becomes E in the cipher text.

The encryption step performed by a Caesar cipher is often considered as part of more complex schemes. When encrypting, the user looks up each letter of the message in the "plain" line and notes the corresponding letter in the "cipher" line. The encryption is represented using modular arithmetic by transforming the letters into numbers first, for e.g.: A = 0, B = 1, C=2,... Z = 25[1]. Ciphering of a letter $x$ by a shift of $n$ can be described mathematically as

$$E_n(x) = (x + n) \mod 26$$

Deciphering is performed similarly,

$$D_n(x) = (x - n)\mod 26$$

Consider an example for above equation. Let the letter ‘B’ (i.e. $x$ in the equation and B=1) be shifted by 3 (i.e. $n$ in the equation). Thus applying the equation we get \((1+3) \mod 26\) = 4. Hence we get the letter having 4 assigned to it i.e. ‘E’.

b) Storing the Key

The secret key (key2) produced after Caesar Cipher method is not encrypted in the first pixel of the image. The pixel value for storing the key 2 is also defined by the user. The pixel value for storing key 2 is completely the choice of the user. The user has to define the pixel number when asked by the software. The number entered by the user is the pixel number which has some value in it. This value is the pixel number of another pixel from which the key2 is to be stored. The entire process is explained by fig.3.

The values indicated are the pixel values. Let the pixel number entered by the user be 3. In the above fig.2 the value at pixel 3 is 25. Thus from the 25th pixel the key2 is being stored.
3) **Encryption Algorithm:**
To perform the steganography of watermarked audio signal and encrypted Image we have used AES standard. The standard is described in detail as follows:

a) **Advanced Encryption Standard (AES Algorithm)**
The Advanced Encryption Standard (AES), also known as Rijndael [3][4] (its original name), is a specification for the encryption of electronic data established by the NIST in 2001. It supersedes the Data Encryption Standard (DES, 1977) [5]. The algorithm of AES is a symmetric-key algorithm [16], which means same key is used for encryption and decryption of the data. AES is based on a design principle of substitution-permutation network. AES operates on a 4x4 column matrix of bytes, known as the state. Some versions of AES have larger block size and may have additional columns. Major AES calculations are performed in a special finite field.

- **Description of Algorithm:**
  1. **Key_Expansions:**
     Through cipher key, Round keys are derived. This is done using Rijndael's key schedule. AES requires a special 128-bit round key block for each round.
  2. **Initial_Round**
     i. **Add_Round_Key**:

     Each block of the round key is combined with each byte of the state by using bitwise XOR.

3. **Rounds**
   i. **SubBytes**

   A non-linear substitution step (Fig.4) is where each byte is replaced with another according to a lookup table.
   
   ii. **Shift_Row**:

   It is a step (Fig.5) where the last three rows of the state are shifted by a certain number of steps cyclically.
   
   iii. **Mix_Columns**:

   It is a mixing operation (Fig.6) which operates on the columns of the state. It combines the four bytes in each column and each state.

   iv. **Add_Round_KEY** (Fig.7)

4. **Final_Round (no Mix_Columns)**
   i. **SubBytes**
   
   ii. **ShiftRows**
   
   iii. **AddRoundKey.**
b) Implementation Algorithm

1. Express the grey-scale image to be encrypted as a two-dimensional matrix whose size is X1 x X2.

\[
\text{Image} = \{\text{Image} (i, j), 1 \leq i \leq X1, 1 \leq j \leq X2\}
\]

2. Convert the two-dimensional Image matrix into a one-dimensional column vector V of length [(X1 x X2):1].

3. Take the pixel number as an input from the sender. The sender pixel value contains another pixel number which stores the secret key. The advantage of this is that, the intended receiver can only know about the pixel value which is entered by the sender. The opponent cannot extract the message due to lack of pixel knowledge where the message is stored.
4. Ask the sender to enter the key (key1). Convert the key1 to a new key (key2) by Caesar Cipher method.
5. Convert the secret code (key 2) in ASCII values. This will produce the hex values of the alphabets which will be useful for hiding.
6. XOR the generated hex values (key 2) with the pixel values of the image (2) where from the message is to be stored. The length of the message should not be greater than the number of pixels of the image2 to be encrypted.
7. Now this Image (2) is used to hide the audio watermarked signal generated above (in point 1. Audio Watermarking) by using AES standard of Encryption.

4) Decryption Algorithm:-

1. Ask the Secret key (1) and pixel number to the receiver. If the value entered by the receiver match with the values entered by sender during encryption read the encrypted image.
2. Perform reverse AES algorithm to obtain the Watermarked sound signal and Image which has secret key (2) embedded in it.
3. Apply Inverse DWT to the watermarked Audio Sound Signal to get the original Sound.
4. Take the LSB of each pixel by performing modulus operation by 2.
5. Now EX-OR each LSB of the pixel with the original image value to get the binary bits of the encrypted key.
6. Express the obtained key in its character equivalent.
7. The key obtained in step 2 is not the same key entered by the user during encryption. It is the cipher of that key.
8. Hence apply de-ciphering to the character equivalent obtained in step 3 to get the original key.

5) Results and Discussion
This section deals with the real time results of encryption and decryption. The original Image shown in fig.8 has no encryption in it. Fig.9 shows the original audio signal. Fig.10 is encrypted Image with the cipher text of the key entered by the sender.

Fig.8: Original Image

Fig.9: Original Audio Signal
6) Conclusion
This work shows the robust method of invisible data hiding technique. Conclusion is that data hiding techniques can be used for a number of purposes other than communication. The invention is free from tampering and hacking since exact knowledge of the hiding scheme is required. The change in the pixel values makes it more relevant and strong to resist the attacks of the opponent.

References
8. Mustapha Hemis and Bachir Boudraa “Digital watermarking in audio for copyright protection” 978-1-4799-8075-8/14/$31.00 c_ 2014 IEEE


