Confidential Communication with the Help of Encryption in Animation Steganography

Sanchit Gaur¹, Rajiv Munjal²

¹Student MTech (cse), C.B.S Group of Institution, Jhajjar, Haryana, India
²Assist. Professor (CSE Dept.), C.B.S Group of Institution, Fatehpuri, Jhajjar, Haryana, India

Abstract: To protect from these undesirable acts, we proposed a new system with use of Steganography and cryptography to make sure high security of the message. One hides the existence of the message and the other distorts the message itself. Here we use one of the most efficient and a secure algorithm is RSA Algorithm for encryption. Animation Steganography is a technique to hide any kind of files into a carrying Animation file. The use of the Animation based Steganography can be more eligible than other multimedia files. In animation embedding text “message” files (that can include power point slides, flash movies, wave files or video files). Animation Steganography is based on two principles. In the first one, the animation can be altered to certain extent without losing its functionality. In second one the host file’s least significant bit can be changed. Animation Steganography is a popular technique of hiding message into animation file. We first encrypt our message and decoy with an efficient algorithm and then hide at random frames in animation.

Key Words: Steganography, Encryption, Cipher, Public Key.

I. INTRODUCTION

Steganography is the process of secretly embedding information inside a data source without changing its perceptual quality. Steganography comes from the Greek word steganos which literally means “covered” and graphia which means “writing”, i.e. covered writing. The most common use of steganography is to hide a file inside another file [1]. Animation Steganography is a technique to hide any kind of files into a carrying Animation file. The use of the animation based Steganography[3] could be more eligible than other multimedia files, because of its size and memory requirements[3]. Here, we use RSA algorithm for message encryption. RSA algorithm is a very secure technique for cryptography. There is a chance to detection of original message after couples of attacks. Therefore, we proposed a new system with combination of steganography and cryptography.

The paper is organized as follows:

Section II describes the proposed approach of this paper.

Section III describes encryption with RSA algorithm.

Section IV describes the popular Steganography technique Animation Steganography.

Section V describes the Experimental results of my above discussed approach.

II. PROPOSED APPROACH

The block diagrams of animation encoder and decoder used to hide and extract the data are given in Figure 1.
The method to embed and extract the hidden message is described as follows. First, we convert original message into cipher text with RSA algorithm. Second, we convert cipher text into binary numbers.

**Encoder**
1. Select the frames from Animation
   a. Converting frames from animation for hiding message and decoy randomly.
   b. RGB frames will be dividing into Pixels for hi.
2. Apply Embedding Algorithm[1]

If C is the value of the bit to be hide and Va is Least Significant bit in the Pixel. Suppose we have 3 pixels in RGB format

<table>
<thead>
<tr>
<th>Pixel</th>
<th>R</th>
<th>G</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>00101100</td>
<td>00011100</td>
<td>11011100</td>
</tr>
<tr>
<td>2nd</td>
<td>10100110</td>
<td>11000100</td>
<td>00001100</td>
</tr>
<tr>
<td>3rd</td>
<td>11010010</td>
<td>10101101</td>
<td>01100011</td>
</tr>
</tbody>
</table>

When the letter A, which binary representation is 01000001 is embedded into the least significant bits of this part of the frame, the resulting grid is as follows:

<table>
<thead>
<tr>
<th>Pixel</th>
<th>R</th>
<th>G</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>00101100</td>
<td>00011101</td>
<td>11011100</td>
</tr>
<tr>
<td>2nd</td>
<td>10100110</td>
<td>11000101</td>
<td>00001100</td>
</tr>
<tr>
<td>3rd</td>
<td>11010010</td>
<td>10101101</td>
<td>01100011</td>
</tr>
</tbody>
</table>

Apply the embedding algorithm we produce an efficient result.

**Decoder**
1. Select the right frames for message extraction.
   a. Select the frames from animation in which message hidden already.
2. Extract the embedding bit by embedding mark.

<table>
<thead>
<tr>
<th>Pixel</th>
<th>R</th>
<th>G</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>00101100</td>
<td>00011101</td>
<td>11011100</td>
</tr>
<tr>
<td>2nd</td>
<td>10100110</td>
<td>11000100</td>
<td>00001100</td>
</tr>
<tr>
<td>3rd</td>
<td>11010010</td>
<td>10101101</td>
<td>01100011</td>
</tr>
</tbody>
</table>

Where, we extract least significant bits of all pixels

**Encrypt message with RSA Algorithm:**
- best known & widely used public-key scheme
- based on exponentiation in a finite (Galois) field over integers modulo a prime
  - nb. exponentiation takes $O((\log n)^3)$ operations (easy)
- uses large integers (eg. 1024 bits)
- security due to cost of factoring large numbers
  - nb. factorization takes $O(e^{\log n \log \log n})$ operations (hard)

**RSA Key Setup:**
- each user generates a public/private key pair by:
  - selecting two large primes at random - p, q
computing their system modulus N=p.q
  note φ(N)=(p-1)(q-1)
selecting at random the encryption key e
where 1<e<φ(N), gcd(e,φ(N))=1
solve following equation to find decryption key d
  e.d=1 mod φ(N) and 0≤d≤N
publish their public encryption key: KU={e,N}
keep secret private decryption key: KR={d,p,q}

RSA Use:
  to encrypt a message M the sender:
    obtains public key of recipient KU={e,N}
    computes: C=M^e mod N, where 0≤M<N
  to decrypt the cipher text C the owner:
    uses their private key KR={d,p,q}
    computes: M=C^d mod N
  note that the message M must be smaller than the modulus N (block if needed)

III. EXPERIMENTAL RESULTS
We are using AVI (Audio Video Interleaved) format animation for hiding message and converting AVI animation into PNG (Portable Network Graphics) format image frames. We are using PNG format because it is lossless data compression we can get real data after compression.

Table I. Configuration Parameters of the Animation

<table>
<thead>
<tr>
<th>Animation Properties</th>
<th>Baseline Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits Per Pixel</td>
<td>24</td>
</tr>
<tr>
<td>Frame Rate</td>
<td>15</td>
</tr>
<tr>
<td>Animation Format</td>
<td>RGB24</td>
</tr>
</tbody>
</table>

Figure 2 the 17th frame of animation rofl.to30second before hide 96 bit message

Figure 3 the 17th frame of animation rofl.to30second after hide 96 bit message
Here, we can see the difference between both histograms it means our message is successfully embedded into frames. PSNR value of above frames before message hide and after message hide is $78.3457$.

IV. FUTURE WORK

An algorithm, which can decide the random positions in the frames and pixels to hide message bits, could be developed. This will further enhance this method of animation Steganography.

V. CONCLUSION

In this paper we presented a way of hiding the secret data inside the cover medium such as animation. The proposed system for data hiding uses RSA for encryption and decryption which generating public key, which results in more secure technique for data hiding. We are using random selection of frames and hide decoy with message also. The strong and weak points of these techniques are mentioned briefly so that researches who work in steganography and steganalysis gain prior knowledge in designing these techniques and their variants. The next plan is to develop a steganography technique that is robust to different types of attacks and the majority of contemporary steganalysis techniques fail to detect the presence of secret messages.

REFERENCES


© 2015, IJARCSSE All Rights Reserved