Secure Data Transmission System Using Cryptography and Video Steganography

Soe Soe Shwe

Lecturer, Information Technology Support and Maintenance Department, University of Computer Studies, Mandalay, Myanmar

Abstract

Today's real transmission environment, two ways for securing message and data are cryptography and steganography. The method of cryptography renders the message unintelligible to outsiders by various transmission methods. On the other hand, steganography is the fine art of hiding the information. Video steganography is a technique to hide any kind of files into a carrying video file. LSB insertion is an important approach for embedding information in a cover video file. To meet the security requirements such as confidentiality and secrecy, this work proposes data security system using LSB based video steganography and digital envelope. The digital envelope is embedded into the cover video file for data security. To create the digital envelope, RC4 and RSA algorithm are effectively combined in the proposed system. The system is implemented by C# programming language.

Keywords - *Cryptography, Steganography, Least Significant Bit (LSB), RC4 stream cipher, Rivest-Sharmir-Adleman (RSA) Algorithm*

I. INTRODUCTION

Steganography is an ancient art of conveying messages in a secret way that only the receiver knows the existence of message. The subject of steganography has been brought into the limelight by several intelligence agencies and the news media in recent times.

Apart from using the state of the art, communication technologies and media, the agencies are using cryptography as well as steganography to aid themselves with their objectives. So, the fundamental requirement for a steganographic method is imperceptibility; this means that the embedded message should not be discernible to the human eye.

Secret information can be hidden in computer image files (JPEG, GIF, BMP), audio files (WAV, MP3) [1], video files (MPEG, AVI), or even text files. Provided the steganographic algorithm is good enough and a stego video along with the original video, even an adept steganography expert would be unable to detect the hidden information from the image. Making use of the Internet, secret information hidden in the carrier can be transmitted quickly, secretly, and securely.

Steganography is not an alternative to cryptography. Steganography is the dark cousin of cryptography. While cryptography provides privacy, steganography is intended to provide secrecy. In other words, cryptography works to mask the content of a message; steganography works to mask the very existence of the message.

A message, either encrypted or unencrypted, can be hidden in a computer video file and transmitted over the Internet, a CD or DVD, or any other medium. The image file, on receipt, can be used to extract the hidden message [2].

In this paper, the message is encrypted using cryptographic encryption algorithms in order to create the digital envelope. To obtain more robust data security system, the digital envelope is also hidden in the video file by using video steganography.

II. RELATED WORKS

In many research areas, video steganography based data security systems are one of the most effective security systems.

In the previous research [2], Mritha proposed modified LSB algorithm for video steganography. This system was designed by embedding text file in a video file (AVI) in such a way that the video does not loose its functionality using Least Significant Bit (LSB) modification method.

Then, Saurabh Singh and GauravAgarwal (2010) presented a novel approach of hiding image in a video. Their proposed algorithm is replacing one LSB of each pixel in video frames [3].

After that, experiment was done by Dr. S.A.K Jilani and A.Swathi (2012) in order to propose a data hiding scheme to hide the information in specific frames of the video and in specific location of the frame [4].

According to the concepts and knowledge pointed out from the previous research works, this work proposes video steganography based data security system. Moreover, video steganography is effectively combined with cryptographic algorithms in order to enhance the security.

III. VIDEO STEGANOGRAPHY AND SECURITY

Since video consists of stream images called as frames, data securing techniques of image will also apply for hiding data in video. Images have a large amount of redundant bits which makes it the most popular cover object for hiding data. Each bit in an image can be encoded to hide information. Information can be hidden in all the pixels of an image or in the selected pixels like in 'noisy 'areas or in the areas where there is a large color variation [5]. Various techniques to hide data in an image are

- Substitution method – Least Significant Bit modification
- Transformation – Discrete Cosine Transform
- Masking and filtering

Among them, LSB coding is very popular and widely used in many information hiding systems such as image, audio and video steganography. In this paper, LSB insertion algorithm is used to hide the digital envelope (combination of encrypted message and encrypted key) into the cover video file.

A. Least Significant Bit Insertion Method

Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover video. Video is converted into a number of frames, and then converted each frame into an image [6]. After that, the Least Significant Bit of some or all of the bytes inside an image is changed to a bit of each of the Red, Green and Blue colour components can be used, since they are each represented by a byte. In other words one can store 3 bit in each pixel. An 800*600 pixel image can store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24 bit image can be as follows:

(00101101	00011100	11011100)
(10100110	11000100	00001100)
(11010010	10101101	01100011)

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

(0010110**0**	0001110**1**	11011100)
(10100110	11000100	00001100)
(11010010	10101101	01100011)

Although the letter was embedded into the first 8 bytes of the grid, only the 2 highlighted bits need to be changed according to the embedded message. On average only half of the bit in an image will need to be modified to hide a secret message using the maximum cover size.

This paper is designed to embed the data (encrypted text) into the video signal and to convert the data into the binary format. Binary conversions is done by taking the ASCII value of the character and converting those ASCII values into binary format and takes the binary representation of samples of cover signal and insert the binary representation of data into that cover signal.

The LSB bits of video signals are substituted by the binary bits of data and this encoded signal is called stego signal is ready for transmission [4].

B. List of File Formats

To create the information hiding system, there are many video file formats. Among them, the widely used video file formats are as follows:

- MOV: Apple Quick Time Movie is a file extension used by the QuickTime-wrapped files [7]. The format was created by Apple Computer to work with multimedia files. MOV is a container format and can contain video, animation, graphics, 3D and virtual reality (VR) content or text.
- ASF stands for Advanced Systems Format. It was developed by Microsoft as part of the Windows Media framework. ASF is most commonly used for streaming media purposes [8].
- MPEG: Motion Pictures Expert Group is the most common implementations of the MPEG-1 standard provide a video resolution of 352-by-240 at 30 frames per second (fps). This produces video quality slightly below the quality of conventional VCR videos [9].
- AVI: means Audio Video Interleave, is a multimedia container format introduced by Microsoft in November 1992 as part of its Video for Windows technology. AVI files can contain both audio and video data in a file container that allows synchronous audio-with-video playback. Like the DVD video format, AVI files support multiple streaming audio and video, although these features are seldom used [10].

In the proposed system, AVI file formats are used as the carrier video file to create video steganography.

IV. OVERVIEW OF CRYPTOGRAPHY

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks (like the Internet). It is the practical art of converting messages or data into a different form, such that no-one can read them without having access to the 'key' [11]. There are several ways of classifying cryptographic algorithms. There are three types of algorithms [12]:

- Seccret Key Cryptography (SKC): Uses a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Symmetric key cryptosystem is illustrated in Figure 1. There are many symmetric encryption algorithms such as AES, DES, Blowfish, RC4, etc.

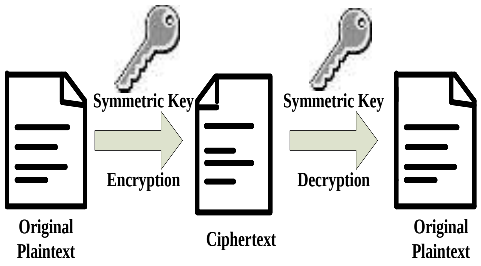

Figure 1. Symmetric key crypto system

- Public Key Cryptography (PKC): Public-key cryptography is also known as *asymmetric-key* cryptography. Encryption and decryption are carried out using two different keys. The two keys in such a key pair are referred to as the public key and the private key [13]. Public key crypto system is illustrated in Figure 2. There are many public key algorithms such as RSA, ECC, etc.

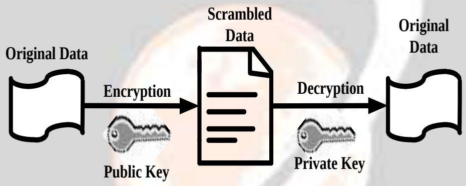

Figure 2. Public key cryptography

- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

In the proposed system, RC4 symmetric encryption algorithm and RSA public key algorithm are used to create the digital envelope for enhancing data security.

V. RC4 Symmetric Algorithm

RC4 is the most widely deployed commercial stream cipher, having applications in network protocols such as SSL, WEP, WPA and in Microsoft Windows, Apple OCE, Secure SQL etc. It was designed in1987 by Ron Rivest for RSA Data Security [14].

RC4 like as a streaming cipher encrypts plaintext one byte at a time, but also can be designed to encrypt one bit a time or even units larger than a byte at a time. In this structure a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are supposed to be truly random. It is combined one byte a time with the plain text stream using the bitwise exclusive-OR (XOR) operation [15].

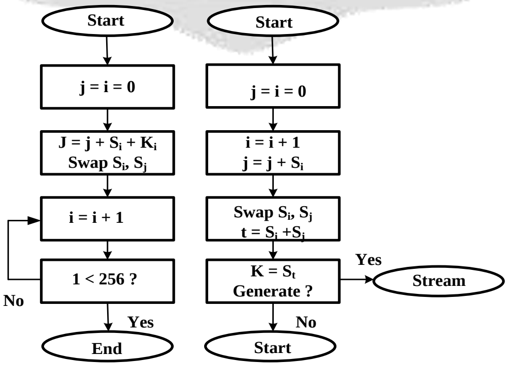

Figure 3. Block Diagram of RC4 Algorithm

The cipher consists of two major components, the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA) [16].

A. Key Scheduling Algorithm (KSA)

The Key Schedule Algorithm of RC4 is presented as follows. It accepts as input the key stored in K, and is 256 bytes long. It starts with the identity permutation in S and, using the key, continually swapping value to produce a new unknown key-dependent permutation.

```
Initialization:
        for i = 0 to 255
        S[i] = i;
        j=0
Scrambling:
        for i = 0 to 255
        j = (j+S[i]+K[i]) mod 256;
        sawp S[i] and S[j];
```

Since the only action on S is to swap two values, the fact that S contains a permutation is always maintained.

B. Pseudo-Random Generation Algorithm (PRGA)

The RC4 key stream generator is presented as follows. It works by continually shuffling the permutation stored in S as time goes on, each time picking a different value from the S permutation as output.

```
Initialization:
         i = 0
         j = 0
Generation Loop:
         i = i + 1
         j = j + S[i]
         Swap(S[i]; S[j])
        Output z = S[S[i] + S[j]]
```

One round of RC4 outputs an n bit word as keystream, which can then be XOR'ed with the plaintext to produce the ciphertext.

C. Encryption and Decryption of RC4

Once the key stream has been generated, the encryption of the plaintext is really simple [17]: it simply consists of a XOR between the plaintext and the key stream. As for the decryption, it is XORed the value K with the next byte of the cipher text.

VI. **RSA PUBLIC KEY ALGORITHM**

RSA algorithm was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978 [18].The RSA scheme is a block cipher. Each plaintext block is an integer between 0 and $n - 1$ for some n, which leads to a block size $\leq \log2(n)$. The typical size for n is 1024 bits. The details of the RSA algorithm are described as follows. The keys were generated as follows.

1. Pick two large prime numbers p and q, $p \neq q$;
2. Calculate $n = p \times q$;
3. Calculate $\_(n) = (p - 1)(q - 1)$;
4. Pick e, so that $\gcd(e, \_(n)) = 1$, $1 < e < \_(n)$;
5. Calculate d, so that $d \cdot e \bmod \_(n) = 1$, *i.e.*, d is the multiplicative inverse of e in mod _(n);
6. Get public key as KU = {e, n};
7. Get private key as KR = {d, n}.

For encryption, plaintext block M< n, its ciphertext $C = M^e \bmod n$ and for decryption, ciphertext block C, its plaintext is $M = C^d \bmod n$.

For this example, the keys were generated as follows.

1. Select two prime numbers, $p = 17$ and $q = 11$.
2. Calculate $n = pq = 17 \times 11 = 187$.
3. Calculate $\varphi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.
4. Select e such that e is relatively prime to $\varphi(n) = 160$ and less than $\varphi(n)$; choose $e = 7$.
5. Determine d such that de K 1 (mod 160) and $d < 160$.The correct value is $d = 23$, because $23 \times 7 = 161 = (1 \times 160) + 1$;

The resulting keys are public key PU = {7, 187} and private key PR = {23, 187}. The example shows the use of these keys for a plaintext input of M= 88. For encryption, one need to calculate C = 887 mod 187=11.

For decryption, it is needed to calculate M = 1123 mod 187=88.

VII. Proposed System Design

The proposed system design is organized with two portions: sender's side and receiver's side as illustrated in figure 4 and figure 5.

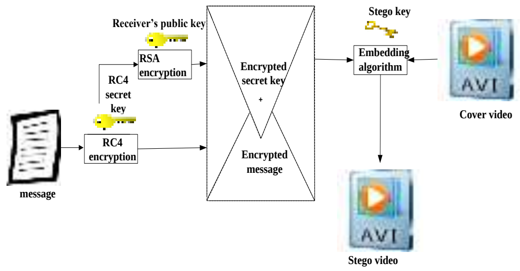

Figure 4. Proposed system design for Sender Site

At the sender's side, the message is firstly encrypted with encryption key (RC4 key) using RC4 encryption algorithm, and then the encryption key is encrypted with the receiver's public key using RSA encryption algorithm to yield a digital envelope.

The encrypted RC4 key and the encrypted messages are represented as a digital envelope as shown in figure 8. After that, LSB embedding technique is used to embed the digital envelope containing encrypted message and encrypted secret key in AVI video file with the help of stego-key in order to obtain stego-video. Then, the user can send the stego-video containing digital envelope to the receiver.

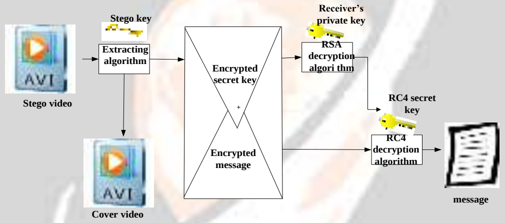

Figure 5. Proposed System Design for Receiver Site

At the receiver's side, the user has to load the stego video. After that, the digital envelope is extracted with the help of stego-key and extracting algorithm from the stego-video as shown in figure 5. Then, the receiver has to decrypt the digital envelope by using RSA and RC4 decryption algorithms to get back the original message.

VIII. Conclusion

In steganography, among the cover files such as audio, video, image etc; videos are the most popular cover objects because the large amount of data can be hidden in the cover file. At the cryptography point of view, the combining usage of symmetric and asymmetric algorithm provides as the strong and efficient information security mechanism. To be more robust in security, the proposed system is focused on video steganography and cryptographic algorithms as hybrid system. This system can only allow (.txt) file format for secret data and (.avi) file format for cover video file. As further extensions, the system can be extended other types of data files and carrier files, such as word document, image files, audio files, etc. Moreover, other cryptographic algorithms can be added according to their security requirements. This system provides secrecy and data confidentiality by using cryptographic algorithms and video steganography. So this system is intended to apply as a strong information security system in the real data communication environments.

References

[1] Mazdak Zamani, Azizah A. Manaf, and Shahidan Avdullah, "A Genetic-Algorithm-Based Approach for Audio Steganography" WASET 2009.

[2] MrithaRamalingam, "Stegomachine – Video Steganography using Modified LSB Algorithm", 2011.

[3] Saurabh Singh, GauravAgarwal,, "Hiding image to video: A new approach of LSB replacement", 2010,6999-7003.

[4] A.Swathi and Dr.S.A.KJilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations",MadanapalliInstitude of Technology and science, 2012.

[5] NavinN.Mittal, "A Video Steganography Model Based on Least Significant Bit Insertion Method", IJCST Vol.3, Issue 2, April-June 2012.

[6] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs: Implementation of LSB Steganography and Its Evaluation for Various Bits, 2001.

[7] http://www.winxdvd.com/resource/mov.htm

[8] http://www.coolutils.com/formats/asf

[9] http://www.webopedia.com/TERM/M/MPEG.html

[10] http://www.winxdvd.com/resource/avi.htm

[11] A. Joseph Rapheal and Dr.V,Sundaram, “Cryptography & Steganography- A Survey”, Vol 2 (3), 626-630.

[12] Gary C. Kessler, “An Overview of Cryptography”, May 1998 (17 November 2006).

[13] Eric Conrad, “Explanation of the Three Types of Cryptosystems”.Mohamed Ali Hashish, “High Performance of RC6 and Twofish”, Feb. 2010.

[14] SouuavSen Gupta, S., Gowtam Paul, S., “(Non-) Random Sequences from (Non-) Random Permutations-Analysis of RC4 Stream Cipher”, FSE, SAC, 2011.

[15] AlaaM.Riad, A., ElminirK.Hamdy, M.,TahaR.Ibrahim, “EVALUATION OF THE RC4 ALGORITHM AS A SOLUTION FOR CONVERGE NETWORKS”,Vol.60,No.3,2009,155-160.

[16] Rick Wash, “Lecture Notes on stream Cipher and RC4”, rlw6@po.cwru.edu.

[17] Quentin Galvane, Baptiste Uzel, “Cryptography-RC4 Algorithm”, February 18, 2012.

[18] Willian Stalling, “CRYPTOGRAPHY AND NETWORK SEURITY-Principles and Practice”, Fifth Addition.

IJARIIE