Grenze International Journal of Engineering and Technology, Special issue

Multilayer Security using RSA Cryptography and Video Steganography

Vennila R[1] and Amudha K[2]
[1-2]Kongunadu College of Engineering & Technology, Department of ECE, Tiruchirappalli, India
Email: venilaraja@gmail.com, amudhak02@gmail.com

***Abstract*—The increased popularity of digital media has raised serious concern over its security-related issue. Security attack in the form of eavesdropping, masquerading and tampering and in many other forms is very common nowadays. Data hiding is one of the rising techniques that aim to provide for security by hiding top secret information into the multimedia contents by varying some nonessential component in the host or cover file. Security of data is very important in a data communication system. Day by day a lot of information is transferred from one user to another on the internet and so the opportunities for data theft also increase. Steganography provides a result for the security of information during any data communication. Data hiding can be done by embedding bits into the LSB parts of R, G and B color spaces, and technique of performing SVD in decomposed DWT submatrices. This approach is similar to sparse representation method, and it can be used for image video steganography. Generally embedding of data can be done directly on the data or can be performed after decomposing the media or by transforming them. Although there are wide varieties of data embedding techniques still these various techniques are vulnerable to attacks, it means there may be a threat to the security of data.**

***Index Terms*— Cryptography, Steganography, RSA Algorithm, LSB video Steganography Algorithm, Information Security.**

I. INTRODUCTION

At present, internet and digital media are getting more popularity. So, the requirement of secure transmission of information also increased. For this reason, a variety of good techniques are proposed and already taken into practices. In this project, I use the steganography process for secure data transmission from the source to destination through the internet**.** Steganography is the method of secretly embedding information inside a video source without changing its perceptual quality. Steganography comes from the Greek word steganos which means "covered" and graphic which means "writing", i.e. covered writing method.

The most common use of steganography is to hide information inside a new file. Generally, in data hiding technique, the actual information is not maintained in its original format. The format is converted into an alternative equivalent multimedia file like images, video or image. This, in turn, is being hidden within another object. Video Steganography is a technique to hide any type of file into a carrying Video file.

The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements are high. The Least Significant Bit (LSB) insertion is the main approach for

Grenze ID: 01.GIJET.5.1.21

embedding data information in a carrier file. Least Significant Bit (LSB) insertion techniques operate on LSB bit of the media file to hide the information bit. In this project, a data hiding method will be developed to hide the information in an exact frame of the video and in a specific place of the frame by LSB substitution using RDH techniques.

II. Overview of Literature

A. Cryptography

Cryptography is a technique for transmitting and storing the data in a particular unintelligible form so that only the intended receiver can read and process it. The reverse process of producing the plaintext back from the ciphertext is called decryption. Cryptographic systems tend to involve both an algorithm as well as a secret value. The secret value is called the key. There are two types of cryptography:

1.Symmetric Key Cryptography:

In symmetric key cryptography, the sender and the receiver agree on a secret key which is used for encrypting and decrypting the messages. The main concern in this type of Crypto-system is a way to share the secret key safely between the two parties. The whole system collapses if the key is known by a third party by any means. Various algorithms that use this mechanism are DES, AES, TDES, and Blowfish.

2. Asymmetric Key Cryptography:

In asymmetric key cryptography, two different keys are used, one for encryption and the other for decryption. This mechanism is also called as the Public Key Cryptography(PKC) since the users use two keys that is, public key, which is known to the public, and private key, which is known only to the user. RSA employs asymmetric key cryptography.

Ron Rivest, Shamir, and Adleman proposed the RSA algorithm. It is a public key cryptosystem which s useful for security in emails and other electronic transactions. Its advantages are: increased security, provides digital signature that cannot be repudiated and large prime numbers can be selected for enhancing the security of keys.

However, the RSA algorithm has some disadvantages as well. The main disadvantage is its speed during encryption [7]. RSA may be vulnerable to impersonation, even if the user's private keys are not available.

B. RSA Algorithm

i. Key Generation

1. Generate two prime numbers randomly that are large, say, p and q and are approximate of equal size.
2. Calculate n = pq
3. phi (ö) = (p-1)(q-1) where n is called the modulus.
4. Choose an integer e, where 1 < e < phi and e are called the public exponent or encryption exponent. The integer e is chosen such that gcd(e, phi) = 1.
5. Compute the secret exponent d, where 1 < d < phi. The secret exponent is also called the decryption exponent. It is chosen such that ed mod (ö)= 1.
6. The public keys are (n, e) and the private keys are (n, d).

ii. Encryption

Suppose A is sending a message to B, then the encryption process involves the following steps:

1. Obtain the recipient's public key (n,e).
2. Represent the plaintext as a positive integer m, where 1 < m < n. If the plaintext is a string of characters then each character is converted into its ASCII equivalent to representing it as a positive integer.
3. Compute the ciphertext c by using the
4. formula: c = me mod n
5. A sender that is A, sends the cipher text c to the recipient B.

iii. Decryption

The recipient B, on receiving the message follows the following steps:

1. Recipient B uses his own private key (n, d) to compute the message representative using the formula: m = cd mod n
2. B then extracts the plaintext from the message representative m. The representative is converted from ASCII to the original message.

C. Steganography

The aim of steganography is to hide top secret information within a cover-media in such a way that others cannot determine the presence of the hidden message. Technically in simple terms ", steganography means hiding one part of data within another".

Steganography, identity-based networks, firewalls, anonymous proxies, and cryptography are the very few major techniques that are employed to achieve secure communication currently. Cryptography is a method of a store and transmits the data in an unintelligible manner so that only the intended recipient or receiver can read and process it. In cryptography, the original message, which is called the plaintext can be converted to an unintelligible form called ciphertext. This is done by using an encryption algorithm. The ciphertext is converted back to the plaintext using a decryption algorithm.

The following media are the candidate for digitally embedding message: -

- Plaintext
- Still imagery
- Audio and Video

III. EXISTING SYSTEM

The existing scheme is made up of image encryption, data embedding, and data-extraction/image-recovery phases. This project uses a separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedding into the encrypted image using a data-hiding key. With an encrypted image contain additional data, if the recipient has only the data-hiding key, they can extract the additional data through recipient does not know the image contented. If the receiver has only the encryption key, they can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data.

The content holder encrypts the original uncompressed image using an encryption key to produce an encrypted image. After that, the data hider compresses the Least Significant Bits (LSB) of the encrypted image using a data-hiding key to create a thin space to accommodate the additional data. At the recipient side, the data embedded in the produced gap can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embed only affect the LSB, decryption with the encryption key can result in an image similar to the original version.

A. Drawbacks

- Difficult to handle large data which are hidden in images
- Video-based reversible data hiding impossible in the existing system
- Increase more LSB panels for hiding

IV. PROPOSED SYSTEM

Present day's transactions are considered to be "untrusted" in terms of security, i.e. they are relatively easy to be a hack and also we have to consider the transfer of a large amount of data through the network will give errors while transfer. A single stage of security is present in the existing systems. The other problem of the existing system is nowadays hacking activities are rising day by day & hacker can easily hack important information's and securities are not sufficient to end hacking. Though security status increased at a higher level the major drawback of a new status of security is cost, it became so costly.

Hence I need enhanced solutions which have good security level at a lower cost. In proposed system is to give an efficient and secure method for video steganography. I make AVI video. The AVI video is big in size but it can be transmitted from a source to target over a network after processing the source video by using these Data Hiding and Extraction procedure powerfully. The proposed methods make an index for the secret information and the index is placed in a frame of the video itself. With the help of this index, the frames containing the secret information are to be found. Therefore, during the extraction practice, instead of analyzing the entire video, the frame containing the secret information is analyzed with the help of index at the in receipt of the end.

The probability of the result of the secret information by an attacker is lesser when compared to the normal method of hiding information frame-by-frame in a sequential way. It also reduced the computational time taken for the extraction process.

A. Advantages

- Reduced Mean Squared Error (MSE)

- Peak Signal to Noise Ratio (PSNR) between the steganography frame and its corresponding cover frame and the PSNR value is calculated to show that the frame is transmitted without any loss or distortion.

V. System Architecture

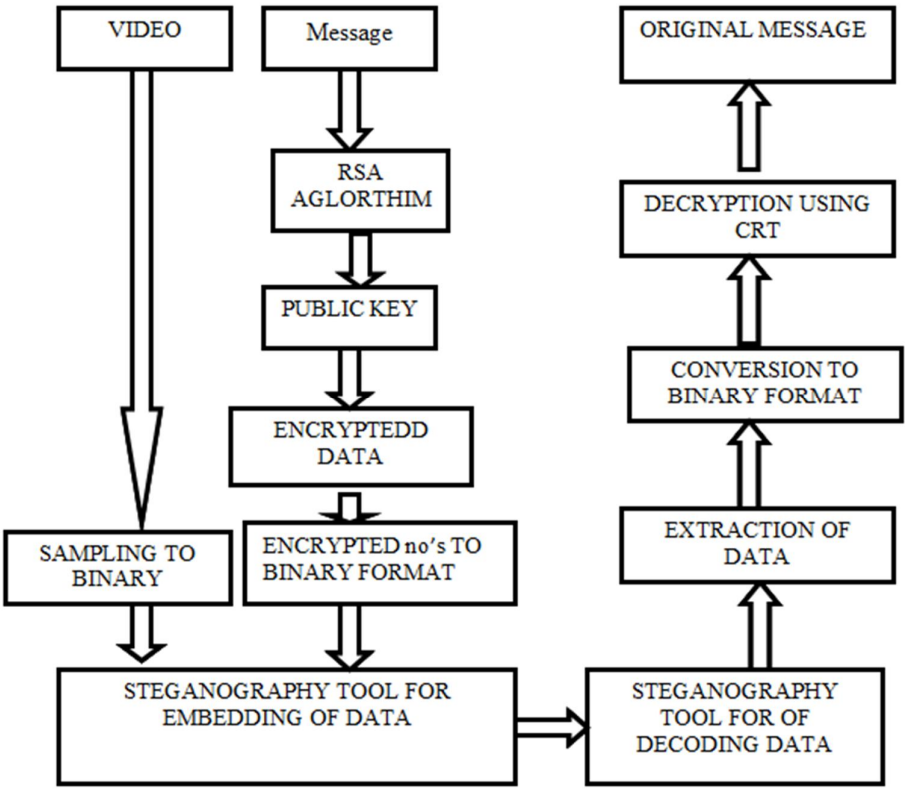

Fig1: Block Diagram of sender and receiver

V. Results

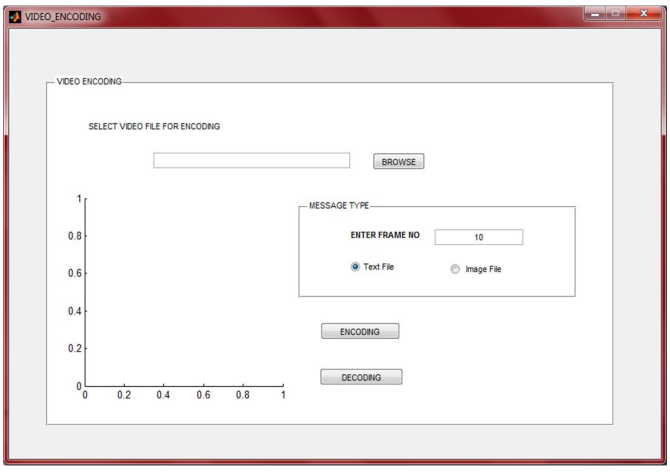

Fig 2: Encoding the video file

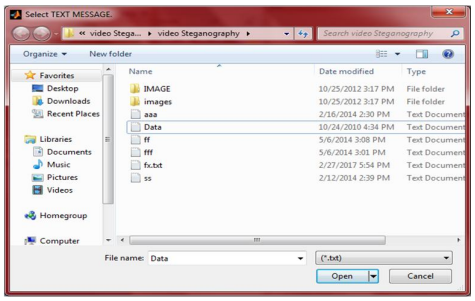

Fig 3: Message selection for embedding with video

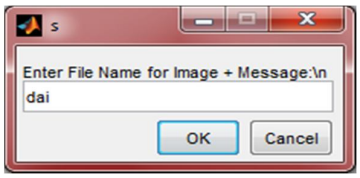

Fig 4: Enter the file name to getting output

Fig 5: Output of hidden message

TABLE I: OUTPUT RESULT COMPARISONS

PARAMETERS	PARAMETER VALUES
PSNR	36.5526
MSE	14.4950
Entropy	7.0140
Standard Deviation	37.0509
Mean	142.9248
Energy	0.2190
Correlation	0.9579
Contrast	0.1182
Smoothness	1.0000

VI. CONCLUSION

Robust algorithms could be developed by integrating two different cryptographic techniques for serving the purpose of preventing cyber-attacks. This algorithm combines the features of both RSA cryptography and video steganography to provide a higher level of security. The proposed technique is implemented using MATLAB. In this technique, first of all, the message is converted to ciphertext by RSA cryptographic algorithm. The ciphertext is then hidden in the video content using the LSB video steganography algorithm. The obtained output video is used as an input video in the second round of video steganography.

REFERENCES

[1] A K Al Frajat, "Hiding data in video file an overview" Journal of applied sciences, vol.10, issue 15, pp.1644-1649, 2010.
[2] Ali K Hmood "An overview on hiding information technique in images" Journal of applied sciences, vol.10, issue 18, pp.2094-2100, 2010.
[3] P Karthigaikumar "Simulation of image encryption using AES algorithm" IJCA special issue on computer science New dimensions &perspectives, vol.7, issue 13, pp.166-172, 2011.

[4] Liu bin, Li Chiang, Li Yao (2005) "Image method based on correlation analysis and image fusion" International conference on parallel and distributed computing, Application and technology, DOI: 0-7695-2405-2/05, 2005.
[5] Marghny Mohamed "Data hiding by LSB substitution is using genetic optimal key permutation" in International Arab journal of e-technology, vol.2, issue 1, pp.11-17, 2011.
[6] P Mohan Kumar and K L Shunmuganathan "A New approach for hiding data in images using image domain method" in the international journal of Computer and internet security, vol.3, issue.12, PP. 69-80, 2011.
[7] Niu Jiping "Image encryption algorithm based on Rijndael S-boxes" in IEEE applied international conference on Computational intelligence and Security, vol.12, issue 7, DOI: 978-0-7695-3508-1, 2008.
[8] Punita Meelu "AES Asymmetric key cryptographic system" in the international journal of information technology and knowledge management, vol.4, issue 7, pp.113-117, 2011.
[9] Saurabh Singh "Hiding Image to Video" International Journal of engineering science & technology, vol. 2, issue 12, pp.6999-7003, 2012.
[10] B Subramanian "Image encryption based on AES key expansion" in IEEE applied second international conference on the emerging application of information technology, vol.11, issue 8, DOI: 978-0-7695-4329-1, 2011.
[11] M Wu, "Hiding in image and video Part I fundamental issues and solutions" IEEE Trans Image processing, vol.12, issue 6, pp.685-686, 2005.
[12] M Wu, E Tang, and B Liu, "Data hiding in digital binary image" in IEEE ICME New York City, NY, USA, vol. 5, issue 13, pp.685-696, 2000.
[13] Balu, S., Babu, C., & Amudha, K. (2016). Enhancing Security and Privacy Authentication for Video Streaming using Data Extracting Video File Selection. Asian Journal of Research in Social Sciences and Humanities, 6(9), 2209-2219.
[14] Amudha, K., Babu, C., & Balu, S. (2016). Enhancing Security and Authentication in Medical Image through ROI based Watermarking Scheme. Asian Journal of Research in Social Sciences and Humanities, 6(6special), 246-258.