ISSN No: - 2456 - 2165

A Novel Technique For Secure Data Transmission Using Cryptography And Steganography

Varsha.S.R.
Computer Science dept. PDA College of engineering
Kalburgi, India
rachottivarsha@gmil.com

Prof. Shailaja Shastri
Computer Science dept. PDA College of engineering
Kalburgi, India
sb_shastri@rediffmail.com

***Abstract*— the main aim of the project is to combine the three independent models such as watermark embedding, data embedding and data extraction into one model. This paper is composed of three parts: watermark embedding, data embedding and data extraction. In watermark embedding model, we are creating the watermarked image by adding watermark data to the original host image using the new fragile watermarking algorithm. The host image may be face, signature or any biometric identification. The result of this will be the watermarked image. The second model is data embedding model, the input of this model is the output of the first model. In this model we are going to add the message or data in a watermarked image through a steganography technique and with the help of secret key. The result of this model is the data with watermarked image; this is known as stego image is transmitted over a channel to the receiver. In the data extraction model, receiver receives the stego image and will extract data. To retrieve data a secret key is required which is embedded in image. This guarantee integrity and confidentiality of the data. One of the applications of our proposed scheme is verifying data integrity for images transferred over the internet.**

***Keywords*—** *Cryptography; Steganography; AES; RSA; Key.*

I. INTRODUCTION

In networking, cryptography can be specified as the security service for data and telecommunications. Cryptography is a primary way to address message transmission security requirements. Encryption and decryption of messages are made for the technique of Cryptography. A mechanism of concealing the original messages from the stranger and by making a suspect of the presence of the message only to the premeditated receiver is called steganography. Here the secret message is sent as image or text through the encryption of the message in which special keys are arranged for those intended receivers to get the original message. The receiver only makes existent procedure of the real message sent by the sender. Real message can be letters or digits which can be encrypted as hidden message in any form as audio or video or image.

Steganography must not be baffled with cryptography, where the message is changed so as to make it's insignificant to vicious people who cut-off. The goal of steganography is to avoid drawing impression to the transmission of the secret message between sender and receiver. A secure data transmission is made using cryptography and steganography. Combination of both techniques results in appearing a highly secured method for data communication.

II. RELATED WORK

In [1] a steganographic scheme was proposed, it uses human vision sensation to hide secret bits. To make this, the secret data firstly are converted into a series of symbols to be enclosed in a notation system with multiple bases. In this case, the particular bases used are resolute by the degree of local variation of the pixel magnitudes in the host image. A change to the least significant bit matching (LSBM) steganography was introduced in [2]. This change provides the desired choice of a binary function of two cover pixels rather than to be random as in LSBM. To increase the level of security, a combined data encoding and hiding process was proposed in [3]. This process was used to overcome the problem of image color changes after the embedding process. The LSB steganography technique is found in [4], it based on embedding the secret message into the sharper edge regions of the image to assure its resistance against image steganalysis based on statistical analysis. A novel image steganography was proposed in [5], it is based on integer wavelet transform [IWT], it is used to embed many secret images and keys in color cover image. A quantization based steganography system presented in [6] embedded the International Journal of Computer Networks & Communications secret message in every chrominance of a color image to increase the hiding capacity. DWT based frequency domain steganographic technique was proposed in [7], the data is hidden in horizontal, vertical and diagonal components of the sub – image. In [8] a secret data communication system was presented, it employs RSA with asymmetric keys and AES with symmetric key to encrypt the data, after that the encrypted data is embedded into the cover image using smart LSB pixel mapping and data transposition method. In [9] and [10] two make sure the communication systems were proposed to be used for voice over IP (VOIP) applications. LSB based steganography was made to hide the information over an audio cover signal. An extended version of SHA-1 (Secure Hash Algorithm) was introduced in [11]; this system can be used to encrypt two dimensional data such as image. It is developed to increase the resistance of image based steganography against the attackers and hackers. A chaotic signal was employed in [12] for image steganography, which presents a scattering format for the embedded data through the cover image. A high capacity and security steganography using discrete wavelet transform (HCSSD) was developed in [13]; the wavelet coefficients for

ISSN No: - 2456 - 2165

the cover image and the payload image were fused to get a single image.

III. PROPOSED WORK

We propose the use of AES (Advanced Encryption Standard), method for the data security which is advised to be the higher level of security by using the multiple data files and key files. It will allow the set of keys at multiple levels to provide highest possible security for the data. In this work, we focus on copyright protection and security issue. The proposed scheme combines the three independent models such as watermark embedding, data embedding and data extraction model into one model. In the watermark embedding model we are embedding watermark data to the original host image using a new fragile watermarking using chaotic sequences, this avoids all weaknesses of the CWSA algorithm. The host image may be face, signature or any biometric identification. The result of this model is the watermarked image. The data embedding model uses the LSB based steganography method to hide the data in a digital image with the help of secret key. The result of this model will be the encrypted watermarked image or stego image. This is transmitted over a channel to the receiver. In the data extraction model the receiver receives encrypted watermarked image. To retrieve the data a secret key is required which is embedded in image. If an unauthorized user tries to access the information from the encrypted watermarked image without a secret key he/she will receives tampered data. Finally it separates the watermarked image and message. This scheme is completely a new concept in the information security using the biometrics, which is a combination of data authentication, privacy and security.

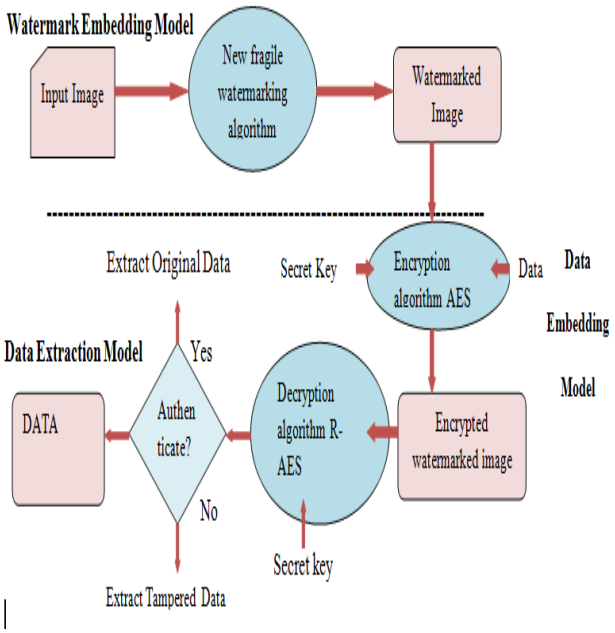

Figure 1: The proposed design

IV. ALGORITHMS

The first message is known as plain text and the encrypted message is called as Cipher text. Encryption is the process of encoding messages or information in such a way that only official parties can read it. This process is done at the sender side which needs a plain text that is to be encoded, a secret key and, an encryption algorithm for fixing the message. While decryption is the process of processing the original message from the encoded one. This is done at receiver side which needs an encoded form of message, a secret key and, a decryption algorithm for coming up with the plain text. The keys which are used to encrypt and decrypt the messages are classified into two forms, Symmetric key (secret key), also called as secret-key cryptography and Asymmetric key (public key) also called as asymmetric-key cryptography.

A. AES Algorithm

AES is the new encryption standard suggested by NIST to renew DES in 2001. AES algorithm can back any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to get the original plain-text. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and arranged as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an AddRoundKey stage. However, before reaching of the final round, this output goes though nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no Mix-column transformation. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns.

Each round of AES is lawful by the following transformations:

1. Substitute Byte transformation

AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte (8-bit) of a data block is converted into another block using an 8-bit substitution box which is known as Rijndael Sbox.

2. Shift Rows transformation

It is a simple byte transposition, the bytes in the last three rows of the state, relies upon the row location, is cyclically shifted. For 2nd row, 1 byte circular left shift is rendered. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively.

3. Mixcolumns transformation

This round is counterpart to a matrix multiplication of each Column of the states. A fix matrix is multiplied to each column vector. In this operation the bytes are taken as polynomials rather than numbers.

4. Addroundkey transformation

It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This transformation is its own inverse.

ISSN No: - 2456 - 2165

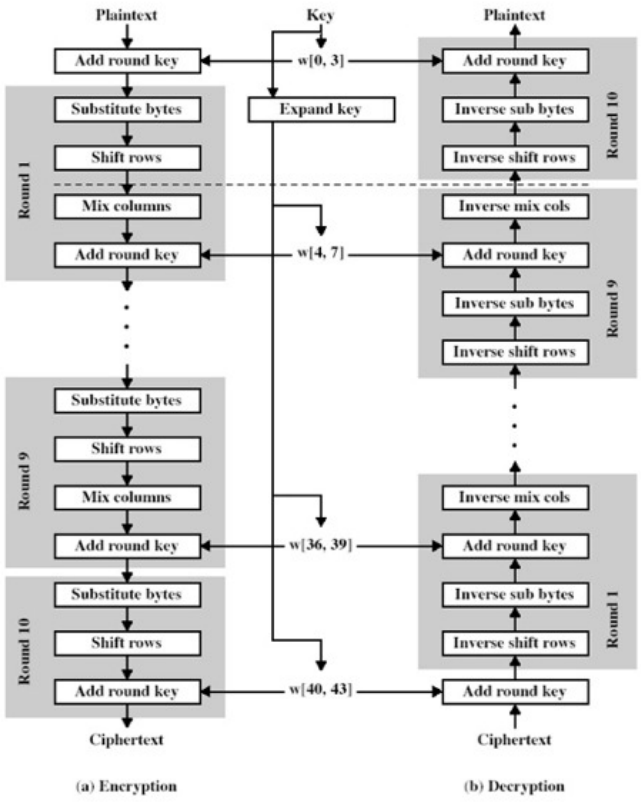

Figure 2: Overall structure of the AES algorithm.

B. RSA Algorithm

RSA algorithm is based on public - key cryptography algorithm which is presented by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is used by modern computers to encrypt and decrypt the messages. It is asymmetric- key cryptographic algorithm which is used for digital signature. The principle of RSA algorithm is "it is easy to multiply prime numbers but hard to factor them". Hence it uses large prime numbers to produce public key and private key respectively, as it usually takes much time.

The steps of RSA algorithm are as follows: -

a) Choose two large prime numbers P and Q (say) such that P is not equal to Q.

b) Calculate N, by multiplying P and Q; N=P*Q.

c) Now to calculate S by formula S= (P-1) *(Q-1).

d) Select a public key e such that e is not the factor of S.

e) Next is to select the private key d such that (d*e) mod S =1.

f) To calculate cipher text (C): $C= M^e \bmod N$.

g) To calculate plain text (M): $M= C^d \bmod N$.

The cipher text is sent to receiver and at receiver side decryption is performed to get plain text.

V. SYSTEM DESIGN

A. Digital watermarking technology

Digital watermarking is a technology for implanting various types of information in digital content. In general, information for protective copyrights and proving the credibility of data is embedded as a watermark.

A digital watermark is a digital signal or pattern attached into digital content. The signal known as a watermark. The digital content could be a still image, an audio clip, a video clip, a text document, or some form of digital data that the creator or owner would like to protect. The main purpose of the watermark is to determine who the owner of the digital data is, but it can also identify the intended recipient.

The Internet boom is one of the reasons. It has become easy to connect to the Internet from home computers and obtain or provide various information using the World Wide Web (WWW). All the information taken care on the Internet is provided as digital content. Such digital content can be easily copied in a way that makes the new file identical from the original. Then the content can be copy in large quantities.

B. Encrytion

Enter the message and converted it into stream. Enter the key file password pair. Starting from zeroth position of the message to the end position, extract bytes corresponding to message stream and XOR them with the key file password pair. The result is considered for steganography. To add more security this resultant stream is reversed. The video is buffered in a local buffer. From the header of video, the length is calculated. The number of message bytes which can be hidden behind each is calculated. Open the independent frames, extract the RGB components of the pixels. Store the length of the message in zeroth pixel of the zeroth frame. The index values are first left shifted and result is XORed with the key file password pair and thus noise added pixels are achieved. The result is stored in a destination video file.

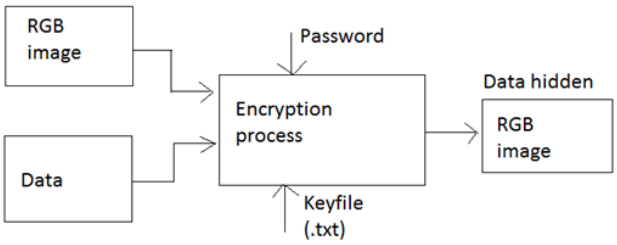

Figure 3: Block diagram for encryption process

C. Decryption

It is just the reverse of encryption. Here the input required is the noisy or text embedded image. Now the image processing says that there exists a relationship between neighboring pixels. The intensity relationship is also called histogram. When text is embedded into the image a lot of noise is obtained. This noise is the desired text. This noise is separated by using low pass filter and histogram shaping. Once the noise is separated this is used to generate characters.

ISSN No: - 2456 - 2165

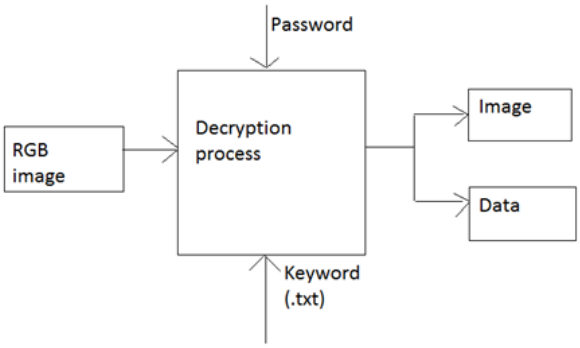

Figure 4: Block diagram for decryption process

VI. COMPARATIVE ANALYSIS

Table 1: comparison between AES and RSA algorithms

S. no	Features	AES	RSA
1	Type of cryptography	Symmetric	Asymmetric
2	Key used	Single key is used	Different key is used
3	Throughput	Very high	Low
4	Confidentiality	High	Low

The above Table 1 describes features of the algorithms used such as the type of cryptography, key used, throughput and confidentiality

Table 2: Time consumed by AES and RSA algorithms when different keys are used.

Sl. No.	Secret text used	Key used	AES (Encryption time) ms	AES (Decryption time) ms	RSA (Encryption time) ms	RSA (Decryption time)ms
1.	Hi how are you	pdaceg	144	115	394	340
2.	Hi this is varsha	Karnataka	162	125	422	360
3.	Varsha. S.R 3PD15SCS20 Pdaceg	information	175	141	442	371

Table 2 shows the secret message, key used for that secret message and followed by time consumed by the AES and RSA for encryption and decryption.

It also describes that as the key length increases the time taken for encryption and decryption also increases.

VII. RESULT ANALYSIS

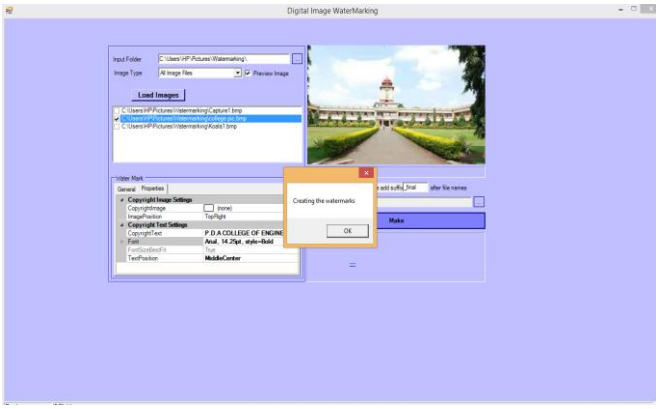

Figure 5: Snapshot of digital watermarking

Figure 5 shows the snapshot of digital watermarking , where we created watermark for certain image.

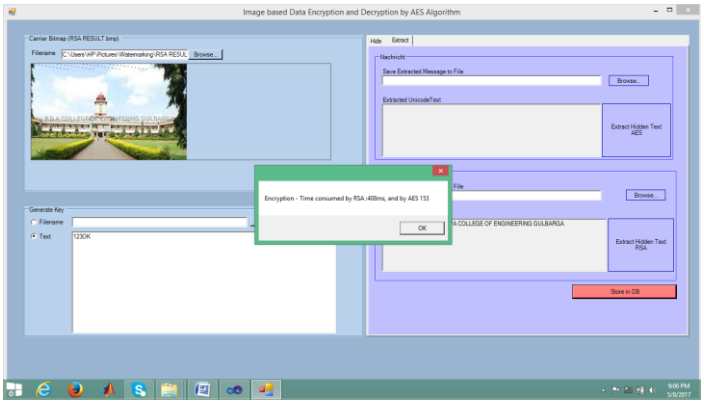

Figure 6: Snapshot of encryption result of both AES and RSA

Figure 6 shows encryption result for AES and RSA which describes that the time consumed by AES is less than RSA that is AES is a faster process when compared to RSA.

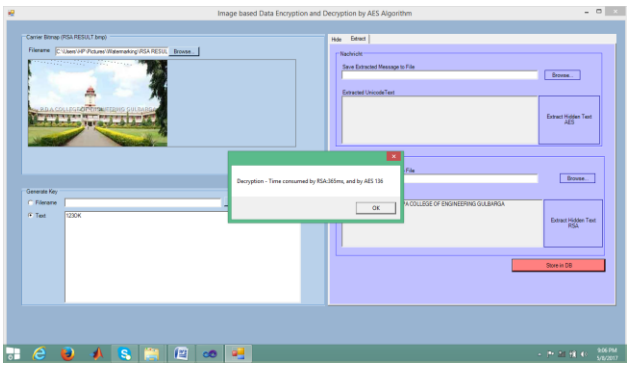

Figure 7: Sanpshot of decryption result of both AES and RSA

ISSN No: - 2456 - 2165

Figure 7 shows the decryption process performed by AES and RSA , which also describes that time taken by AES less when compared to RSA

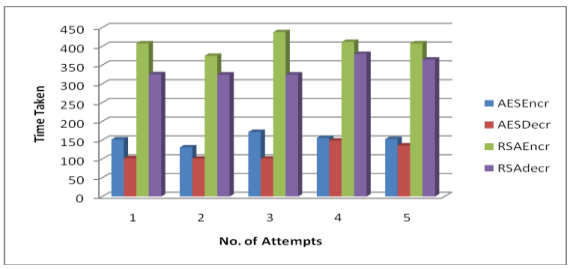

Figure 8: Graph plotted for the no. of attempts performed for both AES and RSA

VIII. CONCLUSION

This paper presents a combination of two different algorithms using Cryptography and Steganography. The collection of these two techniques fulfills the requirements such as highly security and robustness between sender and receiver. The proposed method ensures acceptable image quality with very little distortion in the image.

The goal of this paper is to develop a new security system that messages cannot be retrieved easily from the image by any attackers or hackers in the communication process.

REFERENCES

[1] Xinpeng Zhang and Shuozhong Wang, (2005), "Steganography Using MultipleBase Notational System and Human Vision Sensitivity", IEEE signal processing letters, Vol. 12, No. 1.

[2] Jarno Mielikainen, (2006), "LSB Matching Revisited", IEEE signal processing letters, Vol. 13,No. 5.

[3] Piyush Marwaha, Paresh Marwaha, (2010), "Visual Cryptographic Steganography in images",IEEE, 2nd International conference on Computing, Communication and Networking Technologies.

[4] G.Karthigai Seivi, Leon Mariadhasan and K. L. Shunmuganathan, (2012), " Steganography Using Edge Adaptive Image " IEEE, International Conference on Computing, Electronics and Electrical Technologies.

[5] Hemalatha S, U Dinesh Acharya and Priya R. Kamath, (2012), " A Secure and High Capacity Image Steganography Technique", Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1.

[6] Tong L.and Zheng-ding, Q, (2002), "DWT-based color Images Steganography Scheme", IEEE International Conference on Signal Processing, 2:1568-1571.

[7] Mandal J.K. and Sengupta M., (2010), "Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC).", Proceedings of International Symposium on Electronic System Design, IEEE Conference Publications, pp 225 – 229.

[8] Septimiu F. M., Mircea Vladutiu and Lucian P., (2011),"Secret data communication system using Steganography, AES and RSA", IEEE 17th International Symposium for Design and Technology in Electronic Packaging.

[9] H. Tian, K. Zhou, Y. Huang, D. Feng (2008), "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP", IEEE The 9th International Conference for Young Computer Scientists, pp. 647-652.

[10] Y. Huang, B. Xiao, H. Xiao, (2008), "Implementation of Covert Communication Based onSteganography", IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1512-1515.

[11] Cheddad, A, Condell, Joan, Curran, K and McKevitt, Paul,(2008), "Securing Information Content using Encryption Method and Steganography", IEEE Third International Conference on Digital Information Management.

[12] Rasul E., Saed F. and Hossein S, (2009), " Using the Chaotic Map in Image Steganography", IEEE, International Conference on Signal Processing Systems.

[13] Majunatha R. H. S. and Raja K B, (2010), "High Capacity and Security Steganography using Discrete Wavelet Transform", International Journal of Computer Science and Security (IJCSS),

Vol.3:Issue(6)pp462-472.