A Novel Technique for Secure Data Transmission using Distributed Steganography and Cryptographic Techniques

Smt. K. Venkata Ramana
Department of CSE,
RVR&JC College of Engineering,
Guntur, India

Smt.S. J. R. K. Padminivalli. V
Department of CSE,
RVR&JC College of Engineering,
Guntur, India

Ms. V. Vijaya Lakshmi
HCL Technologies Limited,
India

Abstract— **In this emerging world where individuals seem more valued and powerful, privacy might be under attack and security might be endangered. Security is essential while storing and transmission of information. Cryptography and steganography are two good techniques for data security. In this paper we are proposing a new technique for data security using distributed steganography and public key cryptography. In our proposed technique steganography is used to hide secure data in carrier video, Diffie - Hellman key exchange algorithm is used to produce the keys used for encryption and embedding process and AES is for encrypting the embedding data. The combination of steganography and public key cryptographic technique produces better results for securing the data.**

Keywords— ***Steganography, Distributed Steganography, Information Hiding, Public Key Cryptography, AES, Diffie and Hellman Key Exchange algorithm.***

I. INTRODUCTION

Steganography is the art of concealing the secure messages in other messages [4, 5]. Steganography techniques uses different media like image files, audio files, video files and text files for secret communication [2, 3]. There are many parameters that affect steganography techniques. These parameters include hiding capacity, perceptual transparency (or security), robustness, complexity, survivability, and capability.

Distributed steganography is the process of distributing the secure message across multiple carrier signals or source messages[9]. For example a single text message would be broken into multiple blocks, each block hidden in a different image. The message blocked are permuted according to a key and stored in different carrier messages.

Cryptography is the method that allows information to be sent in a secure form in such a way that the only receiver will be able to retrieve this information [7, 8]. The main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problem like: data integrity, authentication, non-repudiation. Cryptography is divided into two types depending on number of keys used. They are private key encryption techniques and public key encryption techniques. Private key encryption techniques use same key at sender and receiver side whereas public key encryption techniques uses two different keys, one for encryption and other for decryption.

Diffie and Hellman is a public key cryptography technique[10]. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values. In this scheme, there are two publicly known numbers: a prime number q and an integer that is a primitive root of q. Suppose the users A and B wish to exchange a key. User A selects a random integer $X_A <$ q and computes $Y_A = \alpha^{X_A}$ mod q. Similarly, user B independently selects a random integer $X_B <$ q and computes $Y_B = \alpha^{X_B}$ mod q. Each side keeps the X value private and makes the Y value available publicly to the other side. User A computes the key as $K = (Y_B)^{X_A}$ mod q and user B computes the key as $K = (Y_A)^{X_B}$ mod q. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.

AES standards for Advanced Encryption Standard [6]. Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14). These rounds are governed by the following transformations: (i) Byte sub transformation: Is a non linear byte Substitution, using a substitution table (s-box), which is constructed by multiplicative inverse and affine transformation. (ii) Shift rows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes. (iii) Mix columns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers. (iv) Add round key transformation: Is a simple XOR between the working state and the round key. This transformation is its own inverse.

The encryption procedure of AES is: After an initial add round key, a round function is applied to the data block (consisting of byte sub, shift rows, mix columns and add round key transformation, respectively). It is performed iteratively (Nr times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Byte sub, the Inv-Shift rows, the Inv-Mix columns, and the Add round key allow the form of the key schedules to be identical for encryption and decryption.

Steganograhy alone is vulnerable to attackers. If we combine steganography with cryptography it produces better results. In our proposed technique we are using both of these techniques for better security.

II. Proposed Technique

The proposed technique is divided into following steps at the sender side.

- Key generation using Diffie and Hellman algorithm.
- Encrypting the secret data and secret data size using Advanced Encryption Standard.
- Embedding encrypted secret data into video using distributed steganography.

A. Key generation using Diffie and Hellman algorithm:

Diffie and Hellman public key exchange algorithm is used to generate two secret keys- key1 and key2. Each key size is 128 bits. Key1 is used for embedding the secret data into video frames and key2 is used for encrypting the video after embedding process. The complete communication between sender A and receiver B is shown in figure1.Sender and receiver will have some common shared parameters q and α. Each side generates its own private key and calculates public key. Both sender and receiver exchange the public keys. Using the public key of other side and private key of self each side calculates the secret key. This procedure is repeated for producing two secret keys key1 and key2. The terminology used in the algorithm is shown in the table1.

TABLE I. Symbols used in key generation algorithm

Symbol	Description
α	Primitive root
q	Prime number
X_{A1}	Private Key1 of sender
Y_{A1}	Public Key1 of sender
$^{X}{}_{B1}$	Private key1 of receiver
Y_{B1}	Public Key1 of sender
Key_1	Secret key Key1
X_{A2}	Private Key2 of sender
Y_{A2}	Public Key2 of sender
$^{X}{}_{B2}$	Private Key2 of sender
Y_{B2}	Public Key2 of sender
Key_2	Secret key Key2

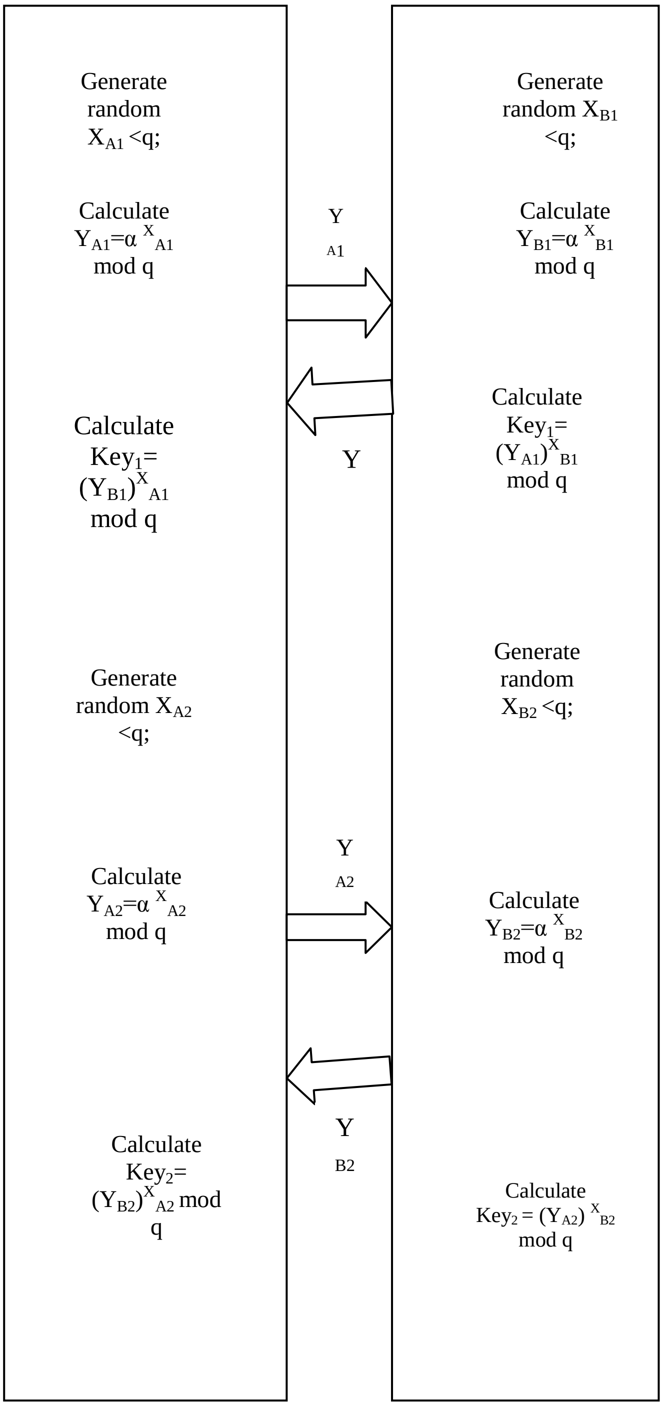
Generate random X_{A1} <q;
Generate random X_{B1} <q;
Calculate $Y_{A1}=\alpha^{X_{A1}}$ mod q
Y A1
Calculate $Y_{B1}=\alpha^{X_{B1}}$ mod q
Calculate $Key_1=(Y_{A1})^{X_{B1}}$ mod q
Y
Calculate $Key_1=(Y_{B1})^{X_{A1}}$ mod q
Generate random X_{B2} <q;
Generate random X_{A2} <q;
Y A2
Calculate $Y_{A2}=\alpha^{X_{A2}}$ mod q
Calculate $Y_{B2}=\alpha^{X_{B2}}$ mod q
Y B2
Calculate $Key_2=(Y_{B2})^{X_{A2}}$ mod q
Calculate $Key_2=(Y_{A2})^{X_{B2}}$ mod q

Fig. 1. Secret keys generation process between sender A and receiver B using Diffie and Hellman key exchange algorithm

B. Encrypting the secret data and secret data size using AES algorithm

Convert the secret data into binary form. Calculate the size of the secret data represent that in 8 bit binary form and append this to the secret data at the starting position. Now encrypt the complete data using AES algorithm. The plaintext for this algorithm is secret data, the key for this algorithm is the Key_2 produced from Diffie and Hellman key exchange algorithm and the cipher text produced is the encrypted data (size +secret data). This data is supplied to the next step for embedding process.

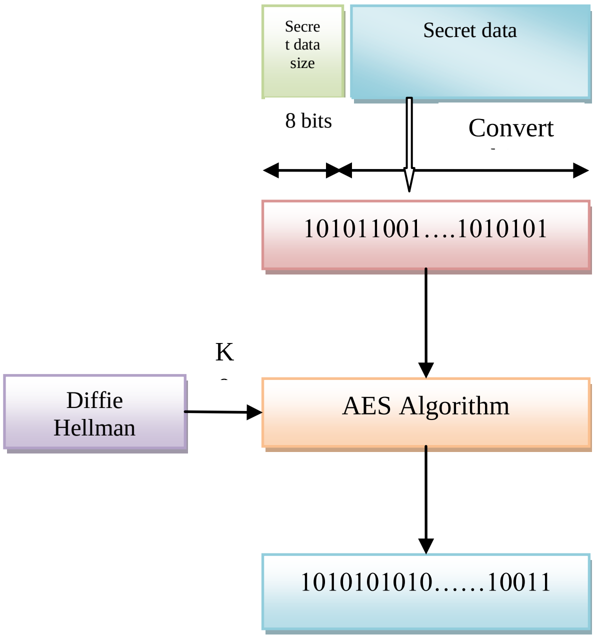

Fig. 2. Encrytion of both secret data and data size usimg AES algorithm

C. *Embedding secret data into video using distributed steganography algorithm*

The steps for embedding the secret data in the video are:

- Consider a carrier video of 64 frames.
- Divide each frame into four blocks of equal size. If frame size is N X M then each block size will be N/2 X M/2.
- Name the four blocks row wise as B_0, B_1, B_2, B_3 in each frame.
- Divide the key key1 into two bit partitions. Name them as ki,j where $1 \leq i \leq 64$. and $1 \leq j \leq 2$. Sub keys $k_{1,1}$ and $k_{1,2}$ is used for embedding data in frame1, likewise $k_{64,1}$ and $k_{64,2}$ is used for embedding data in frame 64.
- The procedure for inserting secret data in each frame is as follows :
- Find the decimal equivalent of first two bits of the key i.e , $k_{1,1}$ and $k_{1,2}$ .Use this number to select a block B_l (where l is equal to the decimal equivalent of $k_{1,1}$ and $k_{1,2}$ and $0<l<3$) in the frame i. For example if $k_{1,1}$ and $k_{1,2}$ bits are 10 then block 2 is selected in the frame 1for inserting data. Using LSB technique insert a bit in each pixel value in the block.
- After inserting the data in frame1 insert the data in frame2 by selecting the random block number using key bits $k_{2,1}$ and $k_{2,2}$.
- Repeat this process for all the frames.
- After inserting data in all the frames, repeat the above process by selecting another block in each frame for the next round.
- For the next round, in each frame block selection is done by adding 1 to the digital equivalent of the previous block number and taking mod by 3. This process guarantees that same block number is not selected in each frame and also blocks selection ranges from 0 to 3. If B_l, is the previous block number select next Bp such that p=l+1 mod 3 and l+1 mod $3 \neq l$ ($0< l+1< 3$, l represents already selected block number for that frame in the previous iteration.
- Repeat this process until all the secret data is completed or all the blocks in each frame are filled. Maximum numbers of complete cycles are 4 because there are 4 blocks in each frame.
- If secret data still remains repeat the process consider second video with the same specifications.

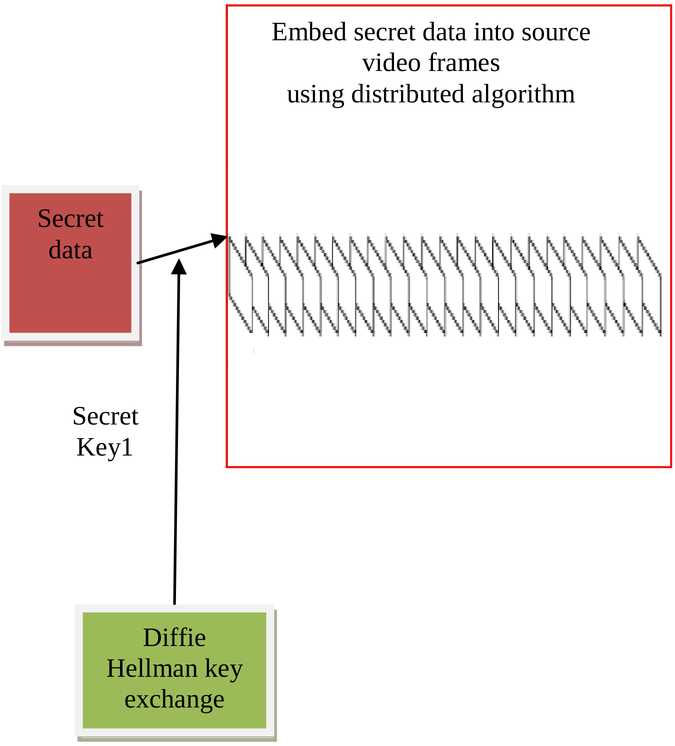

Fig. 3. Embedding of encryted secret data in carrier video frames using proposed algorithm

The video is transmitted to the receiver.

The detailed steps at the receiver side are listed below.

D. Key generation using Diffie and Hellman algorithm.
E. Extracting the encrypted data from the video using distributed steganography.
F. Decrypting the extracted data using Advanced Encryption Standard.

D. *Key generation using Diffie and Hellman algorithm*

This process is the same as the process we have described at the sender side. Receiver by using his own private and public keys produces secret keys key_1 and key_2.

E. *Extracting the encrypted data from the video using distributed steganography*

The steps for extracting the encrypted data from the video :

- Divide the received video into 64 frames.
- Divide each frame into four blocks of equal size. If frame size is N X M then each block size will be N/2 X M/2.
- Name the four blocks row wise as B_0, B_1, B_2, B_3 in each frame.
- Divide the key key1 into two bit partitions. Name them as $k_{i,j}$ where $1 \leq i \leq 64$. and $1 \leq j \leq 2$. Sub keys k $_{1,1}$ and $k_{1,2}$ is used for embedding data in frame1, likewise $k_{64,1}$ and $k_{64,2}$ is used for embedding data in frame 64.
- The procedure for extracting secret data in each frame is as follows :
- Find the decimal equivalent of first two bits of the key i.e , $k_{1,1}$ and $k_{1,2}$ .Use this number to select a block B_l (where l is equal to the decimal equivalent of $k_{1,1}$ and $k_{1,2}$ and $0<l<3$) in the frame i. For example if $k_{1,1}$ and $k_{1,2}$ bits are 10 then block 2 is selected in the frame 1for inserting data. Using LSB technique extract a bit from each pixel value in the block.
- After extracting the data from frame1 extract the data from frame2 by selecting the random block number using key bits k $_{2,1}$ and $k_{2,2}$.
- Repeat this process for all the frames.
- After extracting first block of data from first frame, decrypt the first 8-bits extracted using AES algorithm and find the size of the secret data. This information is used for estimating no of frames and blocks needed to extract further.
- After extracting data in all the frames, repeat the above process by selecting another block in each frame for the next round.
- For the next round, in each frame block selection is done by adding 1 to the digital equivalent of the previous block number and taking mod by 3. This process guarantees that same block number is not selected in each frame and also block selection ranges from 0 to 3.If B_l ,is the previous block number select next Bp such that p=l+1 mod 3 and l+1mod 3≠ l (0< l+1<3, l represents already selected block number for that frame in the previous iteration.
- Repeat this process until all the secret data is completely extracted.

F. *Decrypting the extracted data using Advanced Encryption Standard*

Delete the first 8 bits from the extracted data which represents size of the secret data. Remaining data is supplied to the AES algorithm. This algorithm takes encrypted data as plaintext and produces actual secret data as output. This algorithm uses Key_2 as key for decryption process.

III. IMPLEMENTATION AND RESULTS

A. *Implementation*

We have implemented the proposed algorithm in mat lab using c language. The following is the input secret data we have considered for transmission.

"It was the long still moment when the hedges and borders turned dusky and vague, but anything she looked at closely, a rose, a begonia, a glossy laurel leaf, seemed to give itself back to the day with a secret throb of colour."

This text is converted into binary bit pattern as shown in figure4.

```
      01001001011101000010000001110111011000010111001
```

Fig. 4. Secret data after converted into binary bit stream

We have calculated the size of the above bit pattern and appended it in 8 bits at the starting of the above bit pattern.

We have considered two input videos. One is black and white image and other is color image and implemented our proposed system. The figure 5 shows the snapshot of the first video-video clip, frame1 before and after embedding secret data.

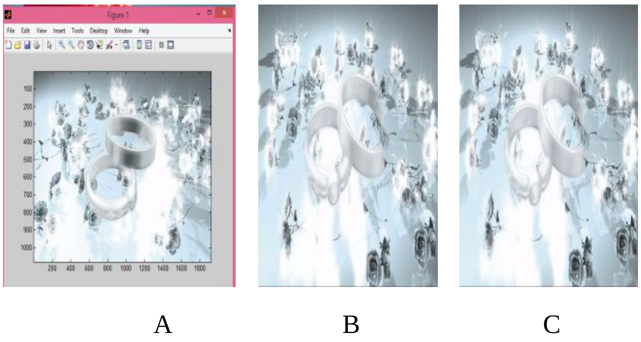

Fig. 5. Snapshot of first video A) Video Clip B) Frame1 before embedding C) Frame1 after embedding

The figure6 shows the snapshot of the second video-video clip, frame1 before embedding and after embedding secret data. We have observed that there is almost zero distortion between the videos before embedding and after embedding processes.

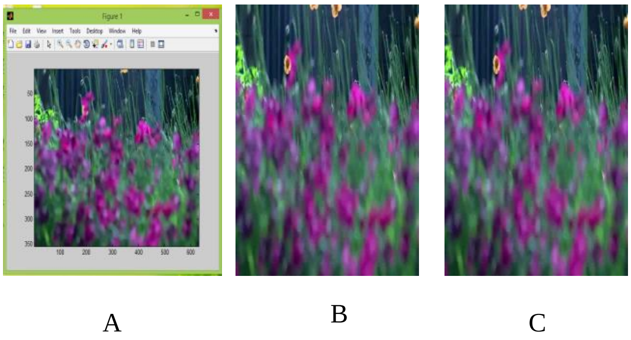

Fig. 6. Snapshot of second video A) Video Clip B) Frame1 before embedding C) Frame1 after embedding

B. *Analysis of results*

We have considered various metrics [1] like- key length in bits, maximum amount of data embedded in single black and white video of size n x m, maximum amount of data embedded in single color video of size n x m, attack steps, attack time in years for evaluating our proposed technique. These metric values for our proposed system are shown below in Table II.

Our Technique is robust against various attacks. The key size is larger with 128 bits for which the brute force attack will take about 1.02 x 10^{18} years for breaking. We have used public key encryption technique Diffie and Hellman to for producing secret keys for encryption and embedding process. This process includes double security with two level keys- private and public keys and secret keys. In the embedding process the complexity of the algorithm still increases because the key is distributed among 64 frames first and then within the frame between four blocks randomly. To add to the complexity we have embedded the encrypted data into the carrier video. The encryption algorithm we have used is AES which requires the attack steps of 2128.We have done the implementation using secret text data, but this method also suits for inserting large data like images and audio.

IV. Conclusion

In this paper we have proposed a new technique for data security. In this technique we have used the concepts of steganography and cryptography which are the two strong pillars of security. By using steganography attackers cannot predict of secure data transmission and by using cryptography attackers cannot understand secret data. We have also used strong public key cryptographic techniques for key generation and embedding processes. The results obtained shows that it is very difficult to predict that some secret data is embedded in the carrier video. The key strength is also very high for the attackers .The future work of this technique can be done by testing this method by embedding image and audio data in carrier video.

References

[1] Norman D. Jorstad , Landgrave T. Smith, “Cryptographic Algorithm Metrics”, January 1997.

[2] Atallah M. Al-Shatnawi, “A New Method in Image Steganography with Improved Image Quality”, Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915.

[3] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).

[4] Yunura Azura Yunus, Salwa Ab Rahman, Jamaludin Ibrahim,“Steganography: A Review of Information Security Research and Development in Muslim World”, American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-11, pp-122-128.

[5] Jasleen Kour, Deepankar Verma, “Steganography Techniques –A Review Paper”, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5).

[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, “A Modified AES Based Algorithm for Image Encryption”, World Academy of Science, Engineering and Technology International Journal of Computer, Information, Systems and Control Engineering Vol:1 No:3, 2007.

[7] Ayushi, “A Symmetric Key Cryptographic Algorithm”, International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15.

[8] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub & Mohammad Odeh, “Survey Paper: Cryptography Is The Science Of Information Security”, International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011.

[9] Liao, Xin; Wen, Qiao-yan; Shi, Sha, “Distributed steganography”, DOI:10.1109/IIHMSP.2011.20.

[10] Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei, Habeeb Omotunde,“Diffie-Hellman and Its Application in Security Protocols”, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012.