Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 6, June 2018, pg.16 – 22

A NOVEL ARCHITECTURE FOR VIDEO STEGANOGRAPHY USING PIXEL PATTERN MATCHING

Chandini B[1], Ganesh Kumar M.T[2]

[1]M.Tech student, G. Madegowda Institute of Technology, Karnataka, India

[2]Assistant professor, Dept. of ECE, GMIT Mandya, Karnataka, India

[1] chandinibalakrishna18@gmail.com; [2] ganeshkmt@rediffmail.com

Abstract— With the strong stimulation of computer networks, computer users increasingly important to find better ways to protect personal and confidential information. A common way to ensure that such information is unreadable string encryption of sensitive data to prevent unauthorized access and viewing. Steganography is the process of hiding confidential data in the media files such as audio, images, videos etc. The point is to plan a steganography calculation which conceal the message behind the picture as well as give more security than others. In the proposed system, the data is encrypted using Advance Encryption Standard and divided using arithmetic division method. In this approach, the data will be stored in the form of divisor, quotient & remainder. The location key is also distributed, encrypted and stored in different frames. Along with this pixel, pattern matching is also used to avoid distortion of the video frame. This system will be difficult to crack since the location key is divided as well as encrypted and stored in different video frames along with this the secret message is stored in the form of a quotient, a divisor and a remainder. Even if the system is attacked the chance of the intruder to predict the pattern will be difficult as the secret data is embedded with dual protection.

Keywords— Advanced encryption standard (AES), Steganography, Pixel pattern matching, Key segmentation

I. INTRODUCTION

Steganography is the science of invisible communication which hides any private data within an innocent looking cover object. The word Steganography is gotten from the Greek words "stegos" signifying "cover" and "grafia" signifying "stating" characterizing it as "secured written work". Steganography is an information hiding technique developed in recent years. Steganography is most frequently related to information hidden with different information in an electronic file. This can be typically done by replacing that least necessary or most redundant bits of information within the original file [11]. Wherever Cryptography scrambles a message into a code to cloud its importance, steganography conceals the message totally. Cryptography works on plaintext to adjust it into indiscernible kind upheld input key. Mystery composing rather works on figure content to recuperate the principal message exploitation the mystery composing key. Video Steganography might be a method to cover any sensibly records into a conveying video document [11] [12].

As exhibited in Fig. 1 Steganography is categorised into four types based on the medium used.

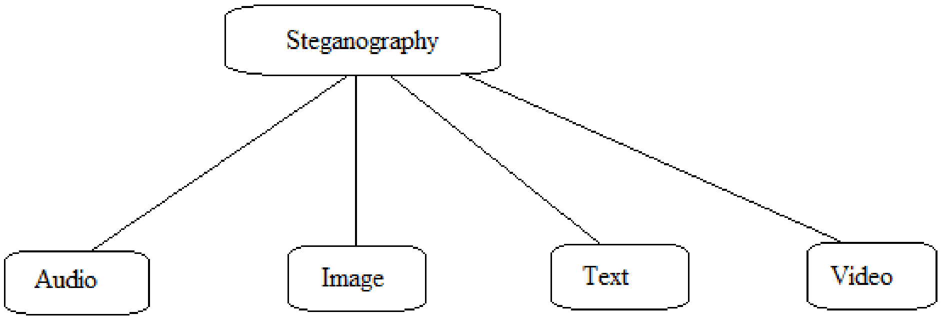


Fig. 1: Types of Steganography

- **Image Steganography-** In this scheme, the information is covered up inside an image file. Images contain much irrelevant information in which the classified data can be implanted efficiently.
- **Audio Steganography-** Here the data is concealed in sound. Secret information is embedded by revising the audio signal so that unauthorized person cannot easily intercept the changes.
- **Video Steganography-** It is a manner to suppress the information in a video file. The pixel variations of the respective frame where the secret data is stored are harder to detect than image steganography.
- **Text Steganography-** This scheme hides the data behind a cover text file.

Develop a system for giving a high security to the text data. Hence the architecture combines both steganography and cryptography. Our project goals are the given below.

- High security to the data.
- Reduce complexity
- High speed
- Reduce the complexity in handling different data base.

II. ADOPTED ALGORITHM

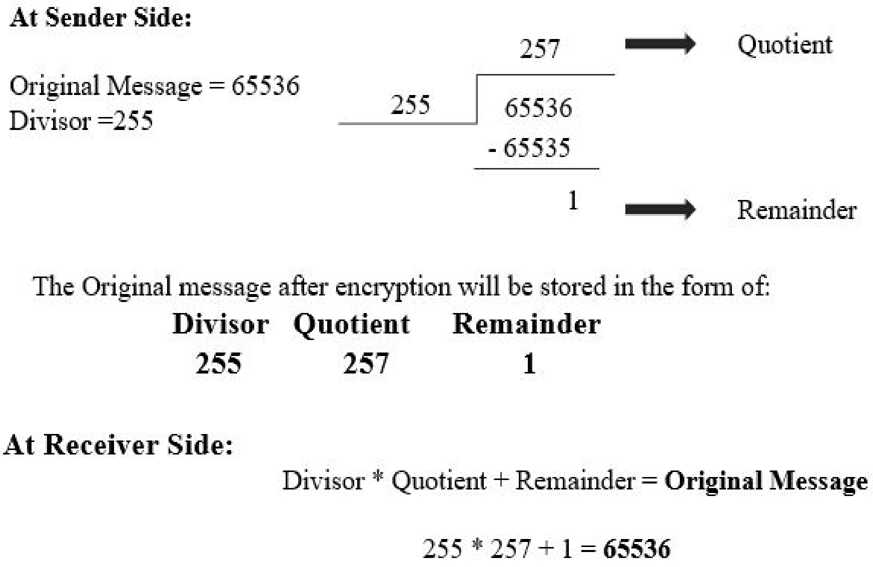
1. AES algorithm

Initially, the secret information is encrypted using AES algorithm. It is a block cipher algorithm which encrypts the data in blocks. It partitions the input into blocks of 128 bits each. It supports the key range of 128 bits, 192 bits and 256 bits respectively. AES being symmetric block cypher technique, for both encryption and decryption same key is used. 10 rounds of operations are performed to the chunk of plain text. These operations consist of substitution, shifting, transposition and shuffling of input message which produces the cipher text.

2. Division method

The output of AES algorithm is then taken as input for this module. Then it is converted into decimal value with the help of ASCII code, this value will act as the dividend. A random number is generated which will be the divisor as exhibited in Fig. 2. The mathematical division is performed with the obtained dividend and divisor. The quotient and remainder of the division performed will be stored in the form of Quotient, Divisor and Remainder in the pixel. And at the receiver side, the data can be retrieved by using the formula:

Divisor * Quotient + Remainder = Message



At Sender Side:

Original Message = 65536
Divisor =255

The Original message after encryption will be stored in the form of:

Divisor	**Quotient**	**Remainder**
255	**257**	**1**

At Receiver Side:

Divisor * Quotient + Remainder = **Original Message**

255 * 257 + 1 = **65536**

Fig. 2. Division Technique

3. Pixel Pattern Matching Technique

Pixel pattern matching is used for embedding the secret data into the frames of a video file. In this algorithm, the data is embedded into the video without changing the original pixel value of the video. Here such pixels are selected from the video whose value matches the data to be embedded. Moreover, the location of these pixels is noted. As in this method, the original pixel value is not altered. As a result, there is no distortion due to the embedding of data [10].

4. Key Segmentation

In the proposed system, the location key is segmented and stored in different video frame. As exhibited in Fig. 3 the address of the embedded pixel is stored in different frames in a linked list fashion.

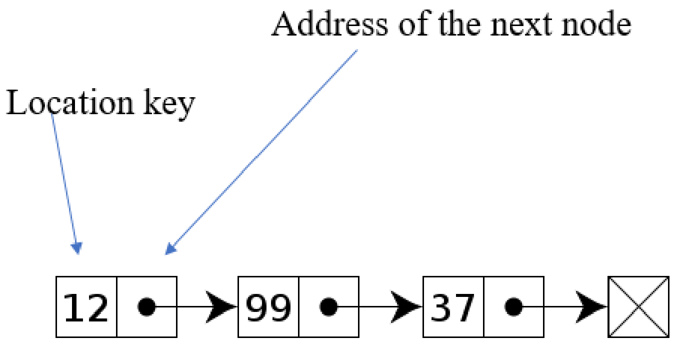


Fig. 3. Division Technique

The flow of linked list method is as follows:

- Initial frame is selected by the system randomly.
- A random pixel in this frame will contain the location of the pixel in which the secret data is embedded and the location of the next node.
- This process continuous until all the location key is stored.

III. PROPOSED METHODOLOGY

The methodology includes two techniques, they are:

A) Encoding Technique
B) Decoding Technique

A) *Encoding Technique*

As exhibited in Fig. 4 the system first takes a secret message from the user. This confidential information is initially encrypted by making use of the traditional AES algorithm. To provide more security, this encrypted secret message is further divided in the form of Quotient, Divisor and Remainder. The system now asks the user for a video file for embedding the data. After the user provides with a video, a random frame is selected where the encrypted message in the form of Quotient, Divisor and Remainder is embedded using Pixel Pattern Matching. As the message is embedded, a location key is generated for each pixel. This location key is embedded in different frames in a linked list fashion using LSB technique. After embedding the secret message and the Location key, a stego video file is generated. This file is then shared with the respective receiver.

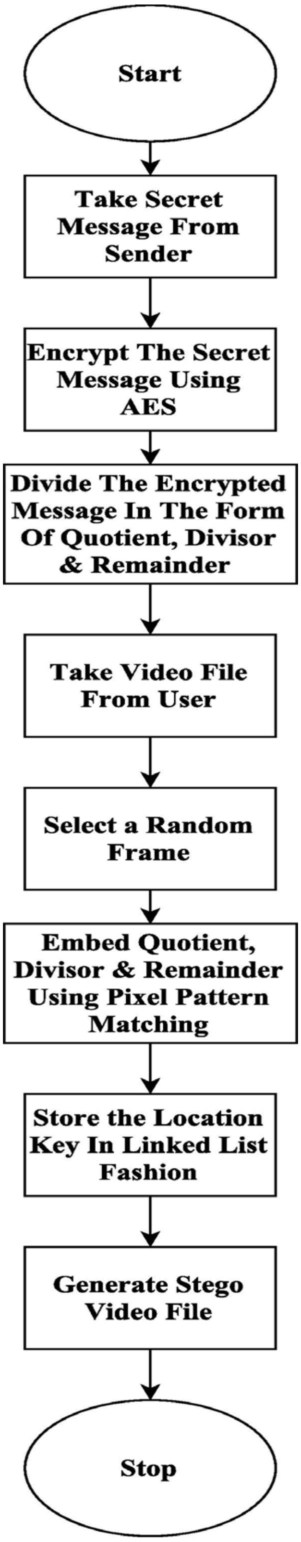

Start
Take Secret Message From Sender
Encrypt The Secret Message Using AES
Divide The Encrypted Message In The Form Of Quotient, Divisor & Remainder
Take Video File From User
Select a Random Frame
Embed Quotient, Divisor & Remainder Using Pixel Pattern Matching
Store the Location Key In Linked List Fashion
Generate Stego Video File
Stop

Fig. 4. System Flow-Encoding

B) Decoding Technique

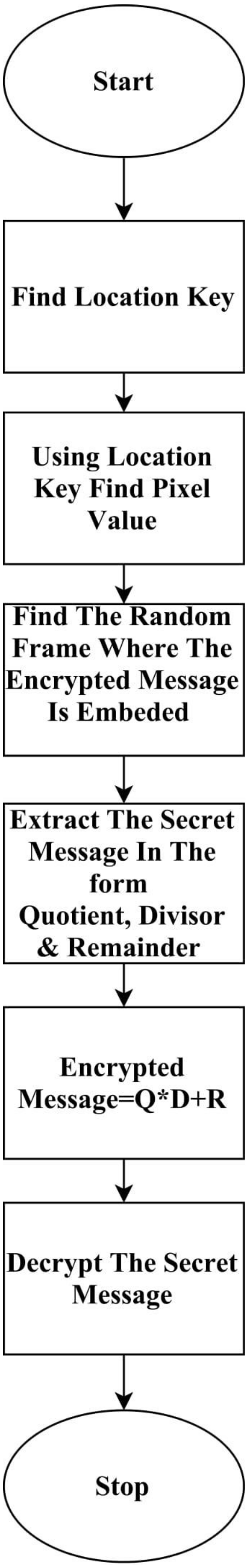

Start
Find Location Key
Using Location Key Find Pixel Value
Find The Random Frame Where The Encrypted Message Is Embeded
Extract The Secret Message In The form Quotient, Divisor & Remainder
Encrypted Message=Q*D+R
Decrypt The Secret Message
Stop

Fig. 5. System Flow-Decoding

As exhibited in Fig. 5 on the receiver end the file when received is scanned for the location key and the random frame where the data is embedded. As the random frame is located the process of extracting the data begins. The value of data bits is found using the location key. Once the data is extracted, it is in the form of Quotient(Q), Divisor(D) and Remainder(R). The Encrypted message is computed using the formula Q*D+R. As the Encrypted message is obtained, the AES encryption is decrypted leaving behind the Original secret message.

IV. RESULT

After embedding the encrypted data into the stego video the results achieved are better than the previous systems in terms of minimum distortion and a negligible increase in file size. Secret message of a significant amount characters can be efficiently embedded into the video frames. As the proposed system make use of pixel pattern matching the distortion is negligible and we can store a significant amount of data into the frame without increasing the video file size. Fig. 6 and Fig. 7 exhibits the frame before and after embedding the encrypted message respectively. As it can be observed, there is no noticeable variation between the two frames.

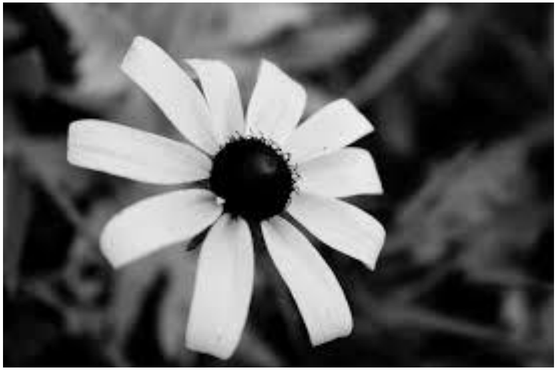


Fig. 6. Frame – Before Embedding

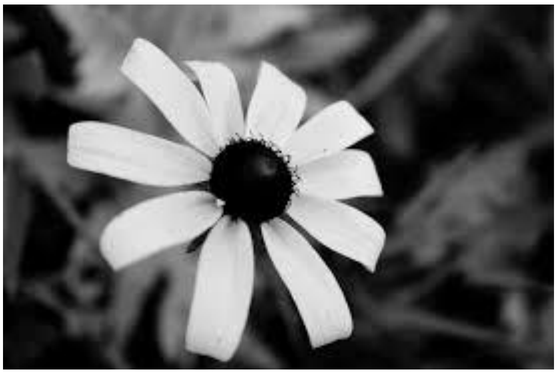


Fig. 7. Frame – After Embedding

Also, the location key is segmented and embedded into the different video frames using linked list fashion. Due to which the retrieval of the embedded data becomes easy and fast at the receiver's end.

TABLE I. RESULTS OF PROPOSED SYSTEM

Original videofile size in(KB)	**Amount of characteristics in secret message**	**Stego video file size in (KB)**	**Result**
5210	100,000	5210	Success
5210	200,000	5210	Success
5210	350,000	5210	Success

Table 1 exhibits the outcomes of the suggested scheme. The initial size of the input video file in KBs is depicted by the first column. The succeeding column depicts the amount of characters that are to be embedded in the video. The 3rd column depicts the size of the video file after embedding the message. The initial size of the video file is 5210 KB and number of character in the message is 100,000, then after employing the proposed scheme, the video size does not have any observable difference. The Result column depicts whether the system successfully decrypted the original message accurately. As a result, the proposed system gives better outcomes than the previous systems.

V. CONCLUSION

The proposed system aims to secure the hidden message by Dividing the encrypted message and then embedding it into the video. Hence the intruder cannot ascertain the presence of concealed message which in turn increases the security. Also, distortion is observed in the systems where encrypting method like LSB is used where data bits are stored in the video frame by manipulating the pixel value. Such distortion is effortlessly perceived by the human eye. Hence the suspicion of secret data stored in video file increases. The proposed system will use Pixel Pattern Matching along with various enhanced encryption and data embedding algorithms to encrypt and embed the secret message, and the location key of the pixels where the information is implanted is stored in different frames. This will result in a safe system with insignificant mutilation so that regardless of the possibility that the intruder gets hold of the stego video they won't be able to get hold of the information. Therefore, the proposed system gives a remarkable approach of covering data in a video with negligible bit distortion.

REFERENCES

[1] R. Patel, A. T. Bhole1, "Steganography over Video File using Random Byte Hiding and LSB Technique", IEEE International Conference on Computational Intelligence and Computing Research, 2012.

[2] N. Bhide, S. Khankhoje, M. Dixit,R. Ukarande, "Video Steganography", Int. Conference on Pervasive Computing(ICPC), 2015.

[3] Pooja,V, Ramandeep K, "A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques", IEEE International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), 2016.

[4] S. Arora, S. Anand , "A proposed method for image Steganography using Edge Detection", International Journal of Engineering technology and Advanced Engineering, Vol.3, Issue 2, February 2013.

[5] H. Gupta, S. Utareja, K. Patel, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Application (0975-8887), Vol. 63-No. 13, February 2013.

[6] R. J. Mstafa,and K. M. Elleithy , "A Highly Secure Video Steganography utilizing Hamming Code (7,4)", Application System, and Technology Conference(LISAT), May 2014.

[7] K. V. Vinodkumar, V. L. Reddy, "A Novel Data Embedding Technique for Hiding Text in Video File Using Steganography", International Journal of Computer Application (0975-8887), Vol. 77 – No. 17, September2013.

[8] R. Balaji, G. Naveen, "Secure Data Transmission Using Video Steganography", IEEE International Conference on 15-17 May 2011.

[9] P. Selvigrija, E. Ramya, "Dual Steganography fo Hiding Text in Video by Linked List Method", Int. Conference on Engineering and Technology(ICETECH), March 2015.

[10] S. Bhat, M.Wagchaude, A. Wadnekar, T. P. Nagarhalli, "Enhanced Steganography Using Pixel Pattern Matching", IEEE Int. Conference on Engineering and Technology(ICETECH), March 2016

[11] Vipula Madhukar Wajgade and Dr. Suresh Kumar, "Enhancing Data Security using Video Steganography", International Journal of Emerging Technology and Advanced Engineering (IJETAC), Vol. 3, Issue 4, April 2013.

[12] Ms. Fameela. K. A, Mrs. Najiya. A and Mrs. Reshma. V. K, "Survey on Reversible Data Hiding in Encrypted Images", International Journal of Science, Engineering and Technology Research (IJSETR), Vol. 3, Issue 4, April 2014.