ISSN [Online]: 2583-2654

Secured Communication and Text Detection of Web Videos

Bhuvaneshwari k
Department of Computer Science and Engineering
Raja Rajeshwari College of Engineering
Bangalore, India
1RR17CS024

Apoorva B
Department of Computer Science and Engineering
Raja Rajeshwari College of Engineering
Bangalore, India
1RR15CS010

Jayanth Kumar Nayak K
Department of Computer Science and Engineering
Raja Rajeshwari College of Engineering
Bangalore, India
1RR156CS048

Bhoomika C
Department of Computer Science and Engineering
Raja Rajeshwari College of Engineering
Bangalore, India
1RR16CS021

Mrs. Devi T
Department of Computer Science and Engineering
Raja Rajeshwari College of Engineering
Bangalore, India

Abstract: This paper focuses on the problem of embedding the text, videos, images and audios. This work aims at helping multimedia content understanding by deriving benefit from textual clues embedded in digital videos. For this, we developed a complete video Optical Character Recognition system (OCR), specifically adapted to detect and recognize embedded texts in videos. Based on a neural approach, this new method outperforms related work, especially in terms of robustness to style and size variabilities, to background complexity and to low resolution of the image. A language model that drives several steps of the video OCR is also introduced in order to remove ambiguities due to a local letter by letter recognition and to reduce segmentation errors.

The internet plays a key role in transferring information or data from one organization to another organization. But anyone can modify and misuse the valuable information through hacking at the time. Steganography plays a very important role in hiding the secret data or information inside the digitally covered information. The hidden message can be text, image, speech or even video. Steganography is a type of cryptography in which the secret message is hidden in a digital picture but here the message, as well as the fact that a secret communication is taking place, is hidden. The hided data can embedded in a video file and it can be extracted in a proper way.

I. INTRODUCTION

Chronic kidney disease (C Steganography find their existence over a long time ago. In past ages Greek Historian Herodotus used to tattoo the secret message over the scalp of the slave and when the hairs were grown again the slave used to dispatched for the destination. During Second World War German discover a new technique called Microdots. In this technique Germans supposed to decrease the size a secret message or image unless and until it will become as the same size of the typed period. Later this technique was used to hide the secret message on a wooden piece and then it is covered by wax. In similar way a new technique were used as invisible ink. In this technique the secret message is written

ISSN [Online]: 2583-2654

with the help of special kind of ink called invisible ink and the message can only be retrieved when the paper gets heated. This technique was also used by Britishers to take charge over India. They supposed to use drum of vaccination to hide. The concept of steganography can be better understood by prisoner's problem. In this problem two prisoners formulate a plan to escape from prison. A warden was appointed to observe their activity. So they supposed to starts communicating in such a way that their communication remains unsuspicious. They used to transmit their message using various cover media.

II. PROPOSED SYSTEM

In this paper, DES, Triple DES and RSA algorithm is used to encode and decode the message with the video.

The user can select the algorithm and encode the secret message in the video file. The destination location is mentioned in the source itself. 4.RSA algorithm will set the secret key before the transmission starts.

III. RELATED WORK

The general architecture consists of two phases:

- Hiding data in Video (Encryption)
- Retrieval of original information (Decryption)

A. Overall Design For Encryption

In Encryption architecture, first the cover converted into a sequence of frames by extracting them. Each extracted frame represents an image. Then the secrete information which has to be embedded inside the video file is first encrypted using Feistel network with different keys (K0, K1, K2 ... Kn). The encrypted information is then separated into bytes of data. Then, each byte of data is embedded into each video frame in a sequence using Linked List Structure Message Embedding Technique. After embedding the information into frames, a sequence of Stego Frames will be obtained. The embedded frames are called as Stego Frame. Later the Stego Frames are combined to get the Stego Video containing the hidden message inside.

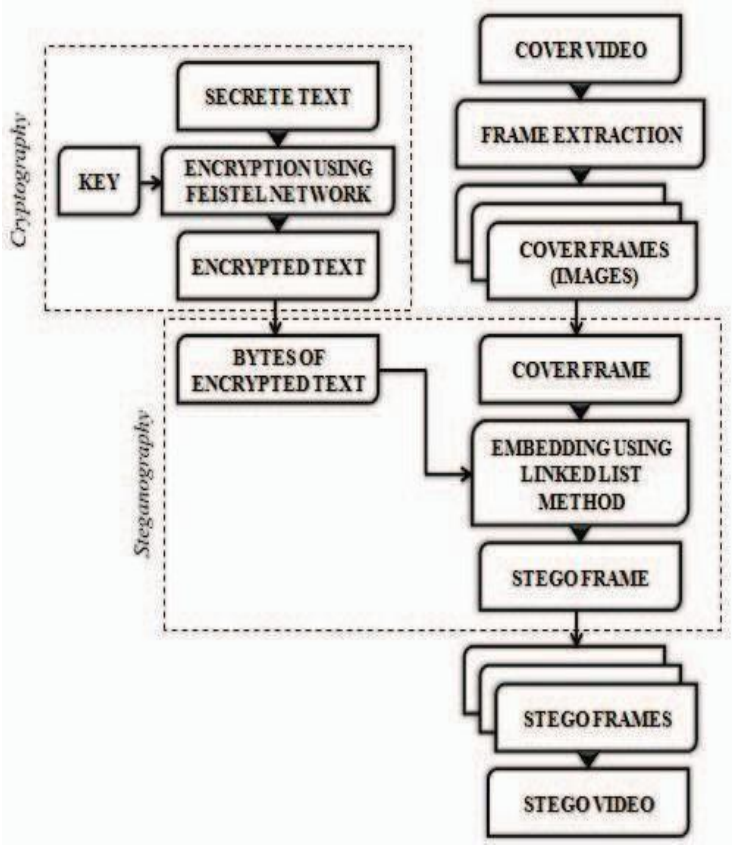

Fig.1.Encryption Architecture

B. Overall Design For Decryption

In Decryption Architecture Fig 2, first the Stego Video containing hidden message is converted into a sequence of Stego frames by extracting them. Each extracted frame represents a Stego image. Then the secrete information is extracted from Stego frames using Linked List Structure technique. The extracted text will be in the form of encrypted message. The message is then decrypted using Feistel Network with various keys (K0, K1, K2 ... Kn) and the original message is obtained. In Decryption Architecture Fig 2, first the Stego Video containing hidden message is converted into a sequence of Stego frames by extracting them. Each extracted frame represents a Stego image. Then the secrete information is extracted from Stego frames using Linked List Structure technique. The extracted text will be in the form of encrypted message. The message is then decrypted using Feistel Network with various keys (K0, K1, K2 ... Kn) and the original message is obtained.

ISSN [Online]: 2583-2654

IV. MODULE DESCRIPTION

The modules are: Encryption process

Decryption process

A. Module 1: Encryption Process

The steps involved in encryption process are:

Extracting frames from video Encrypting data using Feistel network algorithm Embedding text inside image frames Obtaining Stego video

Extracting frames from video

The original video (cover video) is converted into a sequence of frames. Each frame represents an image.

Encrypting data using Feistel network algorithm

The secrete information is encrypted using Feistel network algorithm. In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German IBM cryptographer Horst Feistel; it is also commonly known as a Feistel network. A large set of block ciphers use the scheme, including the Data Encryption Standard (DES).

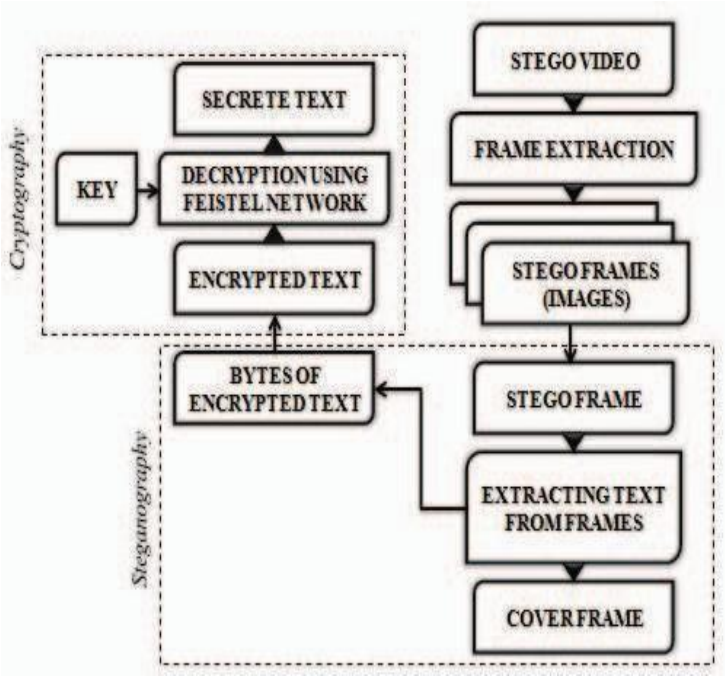

Fig. 2. Decryption Architecture

The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore the size of the code or circuitry required to implement such a cipher is nearly halved. Feistel construction is iterative in nature which makes implementing the cryptosystem in hardware easier. Construction of Feistel Network contains following steps.

1. First split the plain text into two equal pieces, (Lo, Ro).
2. Let F be the round function and for each round i = 0,1,…..,n, compute :

Li+1 = Ri Ri+1 = Li ⊕ F(Ri, Ki)

3. Iterate it till n rounds.
4. Then the cipher text is (Rn+1, Ln+1).

Embedding text inside image frames The text is embedded inside frames using Linked List Structured Message Embedding technique. Here, each byte of the text is hidden in pixels of each frame.

Just after embedding each byte of text, the address of next byte should be inserted in the following pixel.

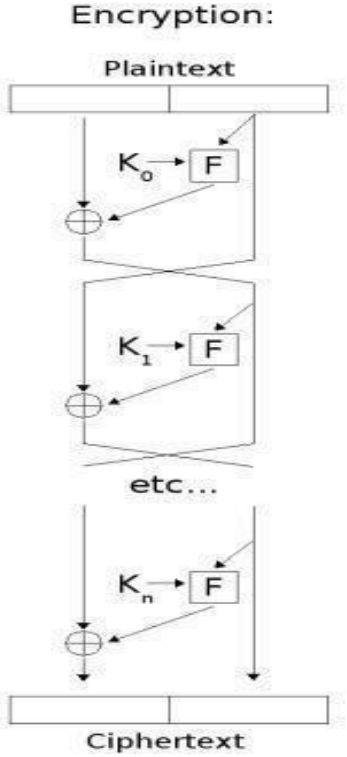

Fig. 3. Feistel Network Encryption

Embedding text inside image frames The text is embedded inside frames using Linked List Structured

ISSN [Online]: 2583-2654

Message Embedding technique. Here, each byte of the text is hidden in pixels of each frame.
Just after embedding each byte of text, the address of next byte should be inserted in the following pixel.

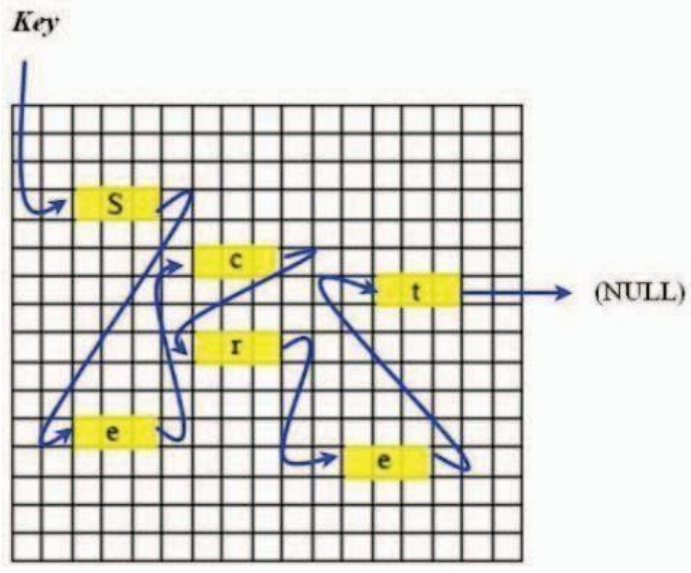

Fig. 4.Embedding a linked list structured message in cover image

Obtaining Stego video

The sequence of images (frames) obtained after embedding process are combined to get a Stego video.

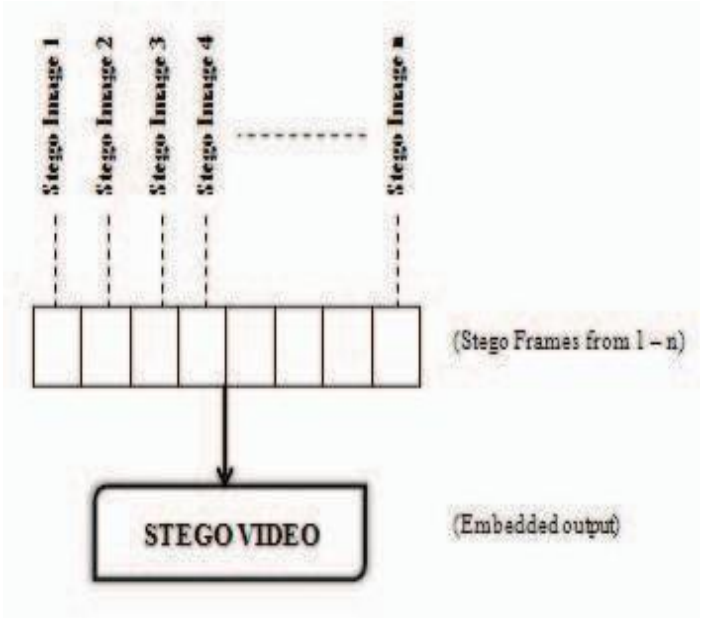

Fig. 5 Stego Video

***B.* Module 2: Decryption Process:**

The steps involved in decryption process are:
Extracting frames from Stego video

Separating data from stego frames
Data decryption to obtain original message

Embedding text inside image frames
The frames are extracted from Stego video as done for encryption process.

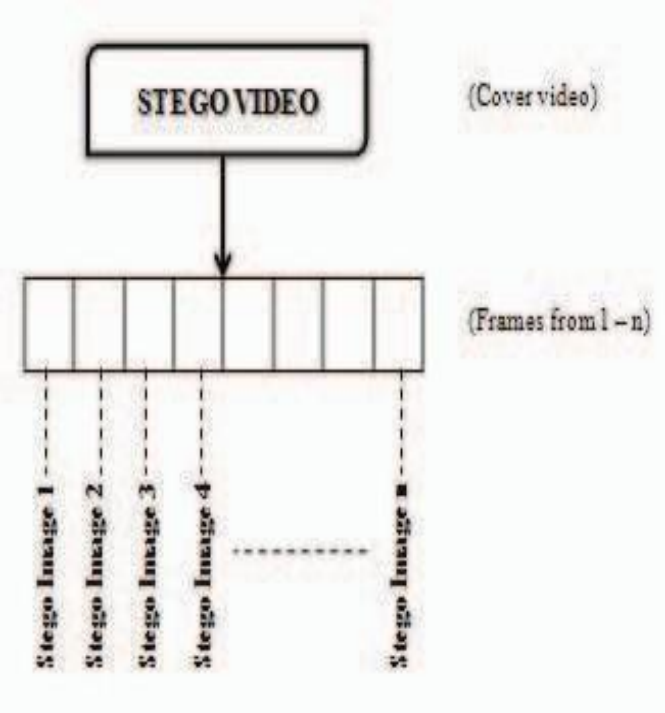

Fig. 6. Extracting frames from Stego video

1) Separating data from stego frames: The information is extracted from stego frames using Linked List Structured Message Embedding technique. The obtained information will be in the form of separated bytes of information. Those parts are joined to get an encrypted text.

2) Data decryption to obtain original message: The decryption of data is done using Feistel Network to obtain the original message.

3) Separating data from stego frames: The information is extracted from stego frames using Linked List Structured Message Embedding technique.
The obtained information will be in the form of separated bytes of information. Those parts are joined to get an encrypted text.

ISSN [Online]: 2583-2654

4) Data decryption to obtain original message: The decryption of data is done using Feistel Network to obtain the original message.

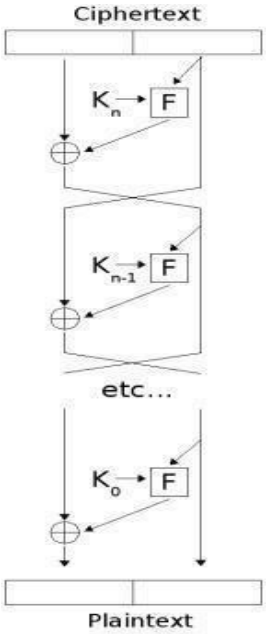

Fig. 7. Feistel Network Decryption

V. EXISTING SYSTEM

In existing system, a generic Bayesian- based framework of Tracking based Text Detection and Recognition (T2DAR) for embedded caption text is first proposed, which performs both tracking based text detection and tracking based text recognition in a single unified pipeline. In general, the feedback information between tracking detection and tracking recognition in complex videos is challenging for exploiting and sharing. In this work, a unified formulation of both tracking based text detection and tracking based text recognition is designed within a Bayesian framework

VI. CONCLUSION

In this paper, the Linked List method and Feistel Network has been introduced for hiding Information inside Video. The two main algorithms used for data encryption and data embedding are Feistel Network and Linked List method respectively. The work begins with extracting frames from cover video. Then the encryption of data takes place using Feistel Network. After encryption of data,the encrypted data is embedded inside each video frames using Linked List method and Stego frames are produced. Later, the tego Frames are combined to get a Stego Video. This technique provides a high level security to the information and the quality of stego video will be equal to the cover video. Since Feistel Network is used for encrypting data, it will be difficult for the intruders to decrypt the information.

Acknowlegment

This work is fully supported by Department of computer science and Engineering from [Raja Rajeswari College of Engineering] through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-III] of the MHRD, Government of India.

REFERENCES

[1] *Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB"), International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.*

[2] *A. Swathi and Dr. S.A.K. Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal of Computational Engineering Research (IJCER), Vol. 2, Issue 5, September 2012.*

[3] Ronak Doshi, Pratik Jain and Lalit Gupta, "Steganography and Its Applications in Security",International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue 6, NovemberDecember 2012.

[4] Rohit G Bal and Dr. P. Ezhilarasu, "An Efficient Safe and Secured Video Steganography using Shadow Derivation", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.

[5] *Hamdy M. Kelash, Osama F. Abdel Wahab, Osama A. Elshakankiry and Hala S. Elsayed, "Utilization of Steganographic Techniques in Video Sequences",International Journal of Computing and Network Technology, Sys. 2, No. 1 Pg. 17-24, January 2014.*

[6] *Hemant Gupta and Setu Chaturvedi, "Video Steganography through LSB Based Hybrid Approach", International Journal of Computer Science and Network Security, Vol. 14, No. 3, March 2014.*

[7] *Anwar H. Ibrahim and Waleed M. Ibrahim, "Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time" ,International Journal of Information Technology & Computer Science (IJITCS), Vol. 7, No. 3, February 2013.*

[8] *Krati vyas and B. L. Pal, "A Proposed Method in Image Steganography to improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 3, Issue 1, January 2014.*

ISSN [Online]: 2583-2654

[9] *Deepak Kumar Sharma and Astha Gautam, "An Approach to hide Data in Video using Steganography",International Journal of Research in Engineering and Technology (IJRET), Vol. 3, Issue 4, April 2014.*

[10] *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.*

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