International Journal of Research Studies in Science, Engineering and Technology
Volume 2, Issue 2, February 2015, PP 34-42
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

Dual Steganography for Hiding Text in Video by Linked List Method

K. Srinivasa Reddy[1], N. Rajasekhar[2]

[1]Associate Professor, Department of Computer Science and Engineering, BVRIT HYDERABAD College of Engineering for Women, Hyderabad, India

[2]Assistant Professor, VNR VJIET, Hyderabad, India

Abstract: *Together with Cryptography the process of using Steganography is called Dual Steganography. Steganography is the practice of hiding a file, message, image, or video in another file, message, picture, or video. Through this, the original videos are protected by applying Dual steganography to it to prevent unauthorized access. In another video the original video is embedded here. Both of the videos are converted to frames at first. The frames of specific video obtained are sampled with those of opposite video frames. Hence encrypted video is obtained by communicating with the output frames.*

Keywords: *Video, Pixels, Linked list, Steganography, secret message, encoding, decoding, hackers.*

1. INTRODUCTION

The analysis of communication, which cannot see all the data inside useless items, is considered to be Steganography. Steganography is subsequent from Greek word ”stegos”, signifying ”cover” and ”grafia”, signifying ”write”, which characterizes it as ”point by point composing”. Steganography is an information search strategy which was created lately. It is a procedure that utilizes human affectability to science and sound to advanced media, and requires classified data in the media to dispatch computerized media, to acquires cretin formation, to accomplish private correspondence. Steganography is not quite the same as cryptography. The objective of cryptography is to bear the cost of secure correspondence by changing the information to an unfathomable structure. Then again, realistic strategies conceal the message itself, making it hard for the third member to discover the content. Not at all like generalizing, sending information is obviously scrambled. So the encryption is certifiably not a decent answer for secure correspondence, however part of the arrangement. These procedures can be utilized together to more readily secure information. The basic model of Steganography Fig 1 appeared in underneath

Model: Hidden Data (D), Carrier(C), Stego Key(K).

1. Message is placed into the cover item that is considered a carrier
2. Hidden details may be any kind of private information that can be plain, figurative or other image material.
3. Key is mainly used to ensure that the solitary recipient with the unraveling key has the option of separating the message from a cover object

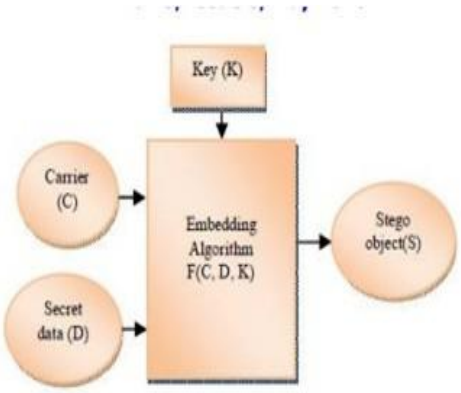

Fig1. *Basic Steganography Model.*

4. The secret data is installed into the cover object by using the embedding algorithm in a way that does not change the first image in a humanly recognizable manner.
5. At long last, the stego object which is the yield of the procedure is the cover-object with the subtly implanted information.

Nevertheless, using encryption for audio records is also another strongest procedure in various systems. Cryptography technique occurs with Audio File to transfer more sensitive touchy data. The delicate message is stored with Video File partner and totally ignored unprotected platforms to complete Systems electively. We now incorporate an inclination for the use of.wav document format for cryptography and Message coding

Using a private key the input video file is embedded with the input message so that the message gets encrypted. The result would be another video document which contains the cryptic information. In order to get the hidden message from it, a similar key should be provided for encrypted video document while decoding.

2. LITERATURE SURVEY

Waleed with the help of Anwar, proposed a Data Concealed in Image Utilizing Steganography: Algorithm and Consequences for the Process encoding and decoding Period. From their vision, organizations, foundations and military frequently have a need to impart a touchy message and consistently convey the threat of catch message by unapproved parties. Use of instant message stowing away inside the image utilizing steganography has all the earmarks of being another of foreseeing the restricted content and limit during implanting and uprooting. This research suggested improvements to the existing methods structure for comparable analysis, using estimates by Robet, Log and many others. It follows these techniques comprehensively by software specification using simulation software for short instant messages, and providing suggestions for these highlights. In wake of breaking down the outcomes canny technique shows the higher stage installing and extraction everything considered the content supplied. It also recommended enhancements to health and offers a truly exceptional kind of steganography.

Astha and Sharma, proposed The Strategy to Mask Video Information Using Steganography. In this, they also suggested a steganographic video replacement formula that typically masks some sort of information or information within the video using a hash function technique. A video steganography is often a method to handle the data beings cattered within the video. Byandlarge, video could be a lot of moving edges, so we here are choosing a casing thus applying a hash work procedure to settle on a pixel for the reason to cover the information. To take the pixel from line and section a double hash function technique is used. It would happen if the pixel in the wake of adding hash power could not be located within the boundary, this sort of problem could arise, and a system of effect targets is used. A equation research approach is used to explain the crash problem where we have a large number with the typical hash appreciation as opposed to straight inquiry. A segment tactic method is used to imply the pixel in a very enclosure which is the area of pixels in line and segment in a such a edge while pixel intensities are revealed, the person of the data to be protected, a parallel approximation of the whole singular individual is overtaken by the red category of unique pixels, at that point the second edge is just to pick and the double value of the second character is to be replaced by the green part of the main pixel, which can continue until each double subject of the information is coveredup.

Hamdy and his team, proposed different strategies for Utilization of Steganographic Techniques in Video Sequences Information security has become the universe of worry as an aftereffects of broad utilization of correspondence medium over the web. When combined with encryption and steganographic strategies besides mystery correspondence, this paper relies on data protection policy by concealing it inside the sight and sound records. The high outcomes are accomplished by giving the assurance to information before transmitting it over the web. The records like pictures, sound, video contains assortment of bits which will be additionally converted into pictures, sound and video. The records made from unimportant pieces or inactive areas that can be used to reformat different information. This paper clarifies the proposed algorithm utilizing video steganography for improving information security.

Ronak Doshi, and his team gave an inside and out clarification on various methodologies towards execution of Steganography utilizing Multimedia records, for example, content, picture, sound and video. Steganography is that the nearest cousin of cryptography, the usage of codes.

While cryptography gives security, steganography is intended to secure the data. Steganography might be a technique for clandestinely conveying. Steganography might be a procedure that includes concealing a message in a suitable transporter for instance an image ora audio document. The bearer would then be able to be sent to a beneficiary without any other individual realizing that it contains a shrouded message. This can be a procedure, which may be utilized for instance by social equality associations in severe states to talk their message to the surface world without their own legislature being alert to it. During this article we attempted to explain the different approaches for using Steganography using the document 'digital technology.' Steganalysis might be a recently rising part of data preparing that looks for the recognizable proof of steganographic covers, and if conceivable message extraction. It's equivalent to cryptanalysis in cryptography. The method is old developing beast that has increased permanent notification since it have recently infiltrated the planet of electronic correspondence security. Objective isn't just to stop the message being perused yet additionally to cover its reality. They additionally clarified the Steganalysis procedure. Steg analysis is the way toward separating the shrouded information by a unauthorized person.

S.A.K. Jilani with his team utilized LSB procedure for concealing data inside the spread video. As indicated by them currently, web and advanced media have gotten increasingly more ubiquity. Thus, prerequisite of secure transmission of information likewise expanded. Hence different great strategies are proposed and as of now taken into training. They used image compression processes during their task for the protected transmission of information from the transmitter to the receiver via the network. Steganographyispre-eminently used regularly to cover a record inside another condensed then on Stego Pictures. document. For the most part, in information stowing away, the specific data isn't kept up in its original arrangement. The arrangement is changed over into an elective equal mixed media records like pictures, video or sound, which progressively is being covered up inside another article. The data would be installed here depending upon its steganographic password. Password with various coefficients is used as polynomial conditions. By utilizing this, the limit of inserting bits in to the duvet picture is frequently expanded Filmasymmetric encryption can be a technique for shielding certain confidential information in a video file. Because of its size and memory needs, the use of video-based data encryption is more qualified than other sight and sound documents. The inclusion of the minimal important component is an invaluable tool for the implantation of data in an excessively bearer paper. Least noteworthy piece (LSB) inclusion method works on media record LSB smidgen to cover the bit of information. During the

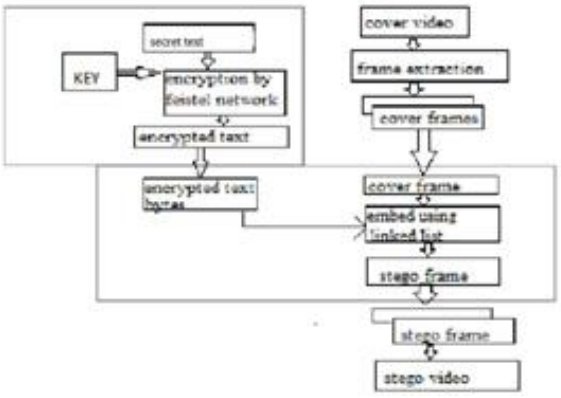

Fig2. *Encryption Architecture whole venture, an information concealing*

plan should be

B. General structure of Decryption

developed to cover the data by using polynomial equation in In the design of Decryption Fig 3 Initially, the steganographic Video obvious clip casings and in explicit casing area by LSB replacement

J.K. Mandal and his team [5] came forward with Hash based Least Significant Bit (HLSB) procedure for inserting mystery data in the involving the hidden message will be transformed into a succession of watermarked frames by removing them. Each separate edge speaks to a frame made by Stego. At this point, the emitting data is removed from Stego frames using the method of Linked List Structure. The separated content would be in bytes of information as encoded message. It is

LSB of the duvet outlines. The Hash Based Least Significant Bit

Technique For Video Steganography tends to hide messages of mystery or details inside a frame. It is only the secured composition that incorporates process that encompasses data inside other information and also hides the very reality that only a then transferred to encoded text. Afterwards the message is unscrambled using Feistel Network with different keys (K1, Kx, Ky ... Km) and the very first text is received.

The total procedure which has occurred during acquiring content mystery text will be sent. Steganography is the art of from stego edge to extricating of concealed information in from of correspondence with mystery, or the study of undetectable bytes and development of a cover frames can be named as correspondence. During this study, a less important component technique for video steganography based on Hash was introduced with the primary aim of injecting mystery data into an incredibly complex video text, thereby splitting it by using a watermarked key or hidden key. In this Least Important Bit inclusion technique is used for steganography and in distributed video information about implants with adjustment within the lower bit is used. The integration of the LSB is notapparent.

3. METHODOLOGY

Data flow diagrams delineate the way the data is stored within a system as well as input and return resources are concerned. It is easy to use information source diagrams to consider giving some market function. The strategy begins with an introductory image of the company and progresses by disintegrating each of the beneficial unmistakably outposts.

3.1. System Architecture

The regular architecture comprises of 2 stages:

steganography and the procedure that has occurred from changing over bytes of information to encoded content and unscrambling to get secret content can be named as the procedure cryptography.

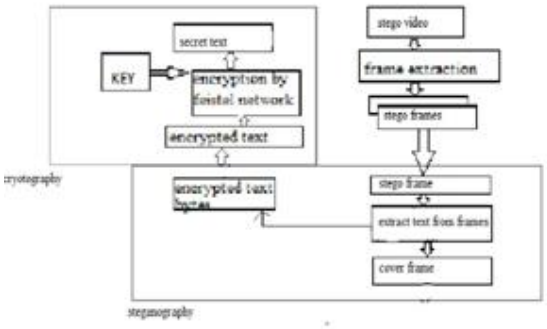

Fig3. *Decryption Architecture*

1) Encryption-Concealing information in Video
2) Decryption-Recovery of actual/initial information

A. General Structure of Encryption

According to the Encryption structure in the Fig 2, Initially the

3.2. Modules

I. Implementation

video is modified by splitting frames into a groups. Every individual frame speaks to a picture, and cover frames are known to be such. At that point, the personal data to be inserted into the clip

document will be scrambled first using Feistel network with different keys (K1, Kx,

... Km). The encoded data was further isolated into input bytes of text. At that point, in an arrangement using connected List composition text Embedding Technique each block of relevant datais

incorporated into every other cover chassis. A grouping of Stego

- Encryptionprocess
- Decryption process

3.3. Module Descriptions

A. Description of Encryptionmodule

The process followed by encryption technique is-

Frames would be gained throughout the lead - up of deploying the information into descriptions. The frames incorporated are named Stego Frame. The Stego Video holding the veiled statement itself is

- Extraction of frames in the video
- Encrypting information utilizing Feistel calculation
- Implanting content within picture frames
- Getting the Stego video

1) Extraction of frames in the video

The initial video is transformed into a frame arrangement. Each frame tells a picture.

Encrypting information utilizing Feistel algorithm

The secrete data is encoded utilizing Feistel calculation. A Feistel code in cryptography is a symmetrical composition used in square figure development, 19th-century german IBM scientist named Horst Feistel; also generally defined as a Feistel n / w A huge Square Figure Arrangement uses the plan along with DES. The Feistel structure has the favorable position that encoding and decoding tasks are fundamentally the same as, even indistinguishable now and again, requiring just an inversion of the key timetable. Along these lines it is about splitting the amount of the program block or hardware components to actualize an estimate. The development of feistel is progressive in nature which simplifies the execution of the crypto algorithm in the equipment. Underneath Fig 4 shows Feistel Network Building with the mentioned advances.

a) Divide the simple contentinitially into the two equivalent parts, let they be Lo and Rorespectively.

b) Then let round process be labeled F, and calculate for every iteration considering different values ranging from 1 to m for

i. now: beginitemize

- Add1toithLtoithR
- Add1toobtainedithRandperformroundfunctionFwith Ri, Ki and multiply withLi

c) Repeat the same m number of iterations.

d) Now the content of a cipher is (Rm+1,Lm+1).

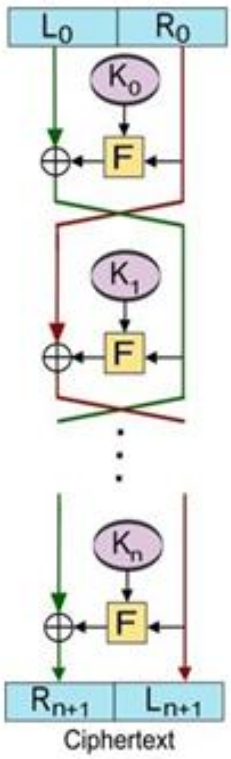

Fig4. *Feistel Network Encryption*

2) Implanting content within picture frames

- The Using the Linked List oriented text compression technique; the content would be installed within the casings. Encrypting data using Feistel approach.
- Here, every byte of the content is covered up in pixels of each casing.
- Only after every unit of information has been inserted, the following byte position will be stored with in corresponding pixel.

- The portrayal of data ought to be as per the following and appeared inFig.5

i) for a byte of data 3 pixels which is 3*3 bytes is allotted

ii) for address of next byte 4 pixels that is 4*4 bytes is allotted.

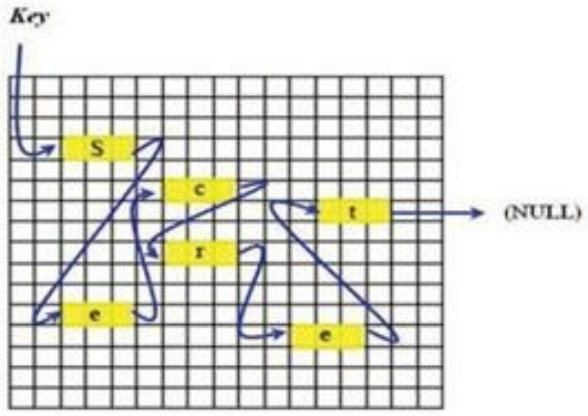

Fig5. *Image describing embedding a cover image witha message*

Getting the Stego video

In the Fig 6, the arrangement of pictures (frames) acquired subsequent to implanting process are joined to obtain a Stego video.

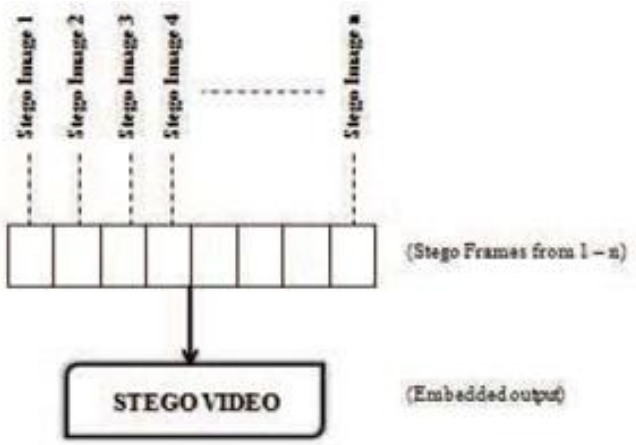

Fig6. *Stego Video*

B. Description of decryption Module

The means associated with decryption procedure are:

- Obtaining the frames from the Stego video.
- Segregating the information from the stego frames
- Decoding of text in order to obtain actual text

1) Obtaining the frames from the Stego video.

The frames are separated from Stego video as accomplished for encryption procedure as appeared in Fig 7

2) Segregating the information from the stego frames:

- Information is extracted from the stego pieces using the centralized text encoding method of Linked List strategy.
- Set of data derived shall be as isolated bytes of data. These are combined to obtain encrypted information

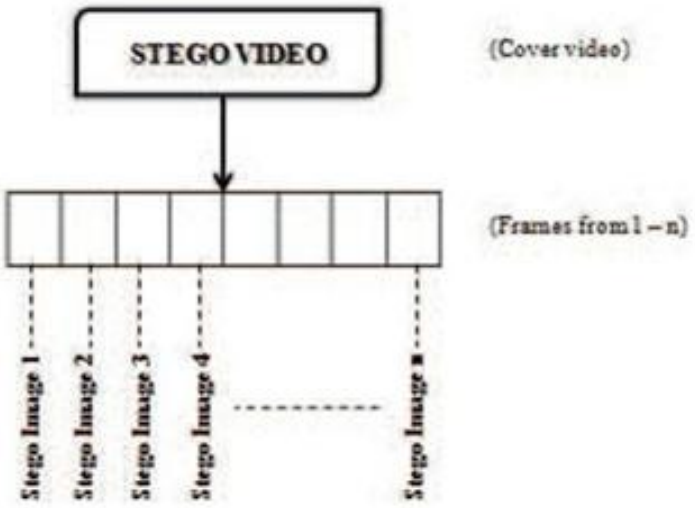

Fig7. *Obtaining frames from Stego video*

3) Decoding of text in order to obtain actual text

Decoding of information is finished utilizing Feistel technique to acquire the first message establishing of steps as appeared in Fig8

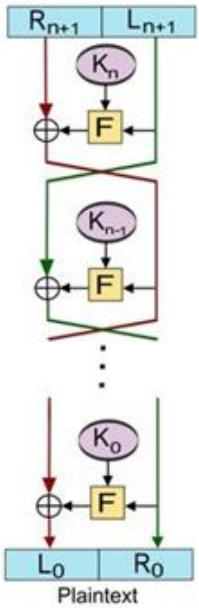

Fig8. *Feistel Network Decryption*

4. CONCLUSION

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

Hamdy M. Kelash, Osama F. Abdel Wahab, OsamaA.

Elshakankiryand Hala S. El-sayed, Utilization of Steganographic Techniques in Video Sequences, International JournalofComputingandNetworkTechnology,Sys.2,No.1Pg. 17-24, January2014

The Linked List procedure along with feistel n/w has been introduced to disguise information within Video. Feistel Network and Linked List methodology are separately the two guideline figures used for information security encryption and data embedding. The work begins with isolating diagrams from spread video. During that moment, data encoding takes place using Feistel Network. After the information is encrypted, the inserted raw data is implanted into each clip outlines using connected List approach and outlines from Stego are provided. The Stego Frames are then merged to obtain a Stego clip. The above technique gave the content a higher level of protection and the essence of stego clip will indeed be comparable to the video spread. As Feistel network is used for information implanting, the data will be difficult for the gatecrashers to unscramble.

REFERENCES

[1] AnwarH.Ibrahimand 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, February2013.

[2] Ronak Doshi, Pratik Jain and Lalit Gupta, Steganography andIts Applications in Security, International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue6, November-December 2012

[3] 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, Issue4, April 2014

[4] Rohit G Bal and Dr. P. Ezhilarasu, An Efficient Safe and Secured Video Steganography using Shadow Derivation, International Journal of Innovative Researchin Computerand Communication Engineering, Vol. 2, Issue 3, March2014.

[5] A. Swathi and Dr. S.A.K. Jilani, Video Steganography by LSB Sub-stitution Using Different Polynomial Equations, International Journal of Computational Engineering Research (IJCER), Vol. 2, Issue 5, September2012

[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] Kousik Dasgupta, J.K. Mandaland 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, April2012.

[8] Krativyas 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.