International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Exploring the Hidden Content from Video Using Data Encryption Standard (DES) Algorithm

Ms.V.Valarmathi[1], Soundarya.B[2], Sumitha.P[3], Sushmitha.R.M[4]
[1]Assistant Professor, [2,3,4]B.Tech Student, Dept Of IT, Prathyusha Engineering College, Chennai,Tamil Nadu, India.

Abstract: ***The rapid development of data transfer through internet made it easier to send data accurate and faster to destination. There are many transmission media like e-mail, chart etc., at the same time it may be easier to modify and misuse the valuable information through hacking.So, in order to send the data securely and without modification, we use an approach like Steganography. This allows the user to hide large amount of information within image or video file. It uses the concept of LSB (Least significant bit) algorithm. This allows us to extract the secret message from the video, as it does not offer flexibility, robustness and high level of security. This project proposes a unique technique for steganography which is based on DES (Data encryption stranded) algorithm.It is a predominant symmetric key algorithm that encrypts the data into the video.It offers flexibility and high level security.This algorithm used to hide the hidden content from the third party.***

I. INTRODUCTION

In today's world communication play a basic need of every growing area.Every one wants to keep the information more safe and secure.In our daily life we use many insecure pathways for transferring and sharing information using internet or telephonically, but sometimes it's not safe. Steganography and Cryptography there are two methods which could be used to sharing information in an encrypted manner. Steganography is a method of information hiding technique. It embeds message into a host medium in order to conceal secret message so as not to arouse suspicion by an eavesdropper. A typically steganographic application includes covert communication between two parties whose existence is unknown to a possible attacker and whose success depends on detecting the existence of this communication. Ingeneral, the host medium used in steganography includes meaningful digital media such as digital image, text, audio, video, 3Dmodel, etc. The receiver is able to extract the message with the help of retrieving process and secret key provided by the sender.

A. Data Security

In data security data has been changed. We implementing a new data security technique is called steganography, it means it doesn't change only the meaning of the data but also change the data from the third party. In this process system is hiding large amount of authenticated data with respect of size, dimension of the image and without disturbing the clarity of the image.

B. Cryptography

The word cryptography is derived from the Greek words "cryptos" which means "hidden" and "graphy" which means "write". The conversion of information into an encryptedformat, rendering it unreadable without the secret knowledge means the cryptography. The process of converting plain text (information) by transforming it into cipher text (unreadable form) is known as encryption. These mathematical schems employ algorithm to actual data into unreadable text or data.

C. Steganography

It is an art which is used to hide some information into other information. Steganography is a science because in today's world we hide secret information i.e., text, audio, video etc. bit wise. Steganography is a technique of hiding secret messages inside a carrier so that only sender and intended recipient of the message known about the presence of hidden message. "Hidden writing" is the actual meaning of steganography which determines the Greek word.

II. LITRATURE SURVEY

A. Texture Synthesis For Mobile Data Communication

This paper (H.Otari and S.Kuriyama) presented in IEEE 2009.This paper presents an approach to image coding that first paints a regularly arranged dotted pattern, using color picked from a texture sample with feature corresponding to the embedded data.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Minimizing Additive Distortion In Steganography Using Syndrome-Trellis Codes

This paper (B.Yang and T.Zeng) presented in IEEE 2011.This paper proposes a complete practical methodology for minimizing additive distortion in steganography with general (non binary) embedding operation. Let every possible value of every stego element by this value. Without any loss of performance, the non-binary case is decomposed into several binary cases by replacing individual bits in cover elements. The binary case is approached using a novel syndrome-coding scheme. Most current coding schemes used in steganography (matrix embedding, wet paper codes, etc.) and many new ones can be implemented using this framework.

C. Image Retrival With Interactive Query Description And Database Revision

This paper (R.J.Anderson and M.G.Kuhn) presented in IEEE 2012.In this paper, an intelligent image retrieval system based on a novel method called database revision (DR) is proposed. Image feature extraction in terms of color, texture and shape is employed to retrieve image from the database. The result of feature similarity comparison of the query image with database images rewrites the database. The system is made interactive for the user to identify the images that are most satisfied to the need. The user-satisfied images are analyzed and the database is revised to make the system intelligent.

D. Video Synthesis With Multi-Frame LBP-Top And Diffeomorphic Growth Model

This paper(Y.Guo,G.Zhao,Z.Zhou and M.Pietikainen) presented in IEEE 2013.Video texture synthesis is the process of providing a continuous and infinitely varying stream of frames, which play an important role in computer vision and graphics. It still remains a challenging problem to generate high-quality synthesis result. It aims to establish a diffeomorphic growth model to emulate local dynamics around stitched frames. The proposed approach is thoroughly tested on public database and videos from the internet, and is evaluated in both qualitative and quantitative ways.

E. Local Prediction Based Difference Expansion Reversible Watermarking

This paper (I.C.Dragoi and D.Caltuc) presented in IEEE 2014.This paper investigates the use of local prediction in difference expansionreversible watermarking. For eachpixel, a least square predictor is computed on a square block centered on the pixel and the correspondingprediction error is expanded. The same predictor is recover at the dection without any additional information.

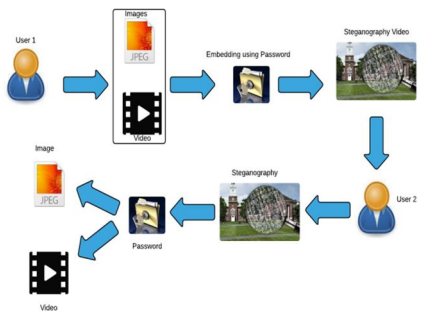
III. EXISTING SYSTEM

The existing system of most of the steganography is LSB algorithm. This means Least Significant Algorithm. In LSB algorithm, the message bit is taken from the message byte and then that particular bit will be embedded inside the least significant bit of an image or video or audio file. However, thereis few weakness of using LSB. It contains disadvantages like low robustness to malicious attack. Vulnerable to accidental or environmental noise. Low temper resistance.

IV. PROPOSED SYSTEM

In this proposed, we use DES (Data Encryption Standard) algorithm to embed the data. This algorithm is better than LSB algorithm.by using this method it increases the value than other methods. This method provides the security to the secret messages. It contains advantages like user friendly. Resistance to brute force attack. Eliminate security issues.

V. SYSTEM ARCHITECTURE



VI. MODULES

A. Secret Message Formulation

Secret message formulation is, out secret message which is an image. A pixel value of first 8*8 of 128*128 sized image is taken in. Each pixel intensity is then converted into equivalent binary values. As the size of the image is 128*128 we got 128*128=131072 bit (the secret message bits to be hidden).

B. Frame Extraction And Embedding Secret Message

Here we have taken an AVI video file as a cover or host video and all frames are extracted (28 frames). The R-channel is used for encoding secret message after preforming blocks DCT on those frames. Here we embed 16 bits per 8*8 DCT higher order coefficient and in a particular frames we can embed frames can accommodate our secret message bits. After extracting the frames, each R-channel frames is block processed by 8*8 DCT and 16-bit secret message bits are embedded into the higher order DC coefficient of each block. After encoding the R-channels of frames we combine those to get the video AVI file with secret message embedded.

C. Decoding And Reconstruction Of Secret Message

Decoding is done in reverse way of encoding.
Step 1: First video frames are extracted.
Step 2: R-channel frames are processed by 8*8 block DCT.
Step 3: 8*8 block processed R-channel original frame values are subtracted to get secret message.
Step 4: From extracted secret message the image is reconstructed.

D. Key Encryption

In this module, when the user wanted to hide the image in video can have password key encryption. So that the image will get hide in video by encryption password. Besides, if the user wanted to unhide the image from the video, need to put the encryption password to get the image video.

VII. CONCLUSION

In this paper, a DES (Data Encryption stranded) algorithm is used. This paper reviewed the new field of steganography. In future there are several directions with this method. By using this method it provides us to get the clear data information from the sender and also provide high security for the data.

REFERENCES

[1] I.C.Dragoi and D.Caltuc, “Local Prediction Based Difference Expansion Reversible Watermarking”, 2014.
[2] Y.Guo, G.Zhao, Z.Zhou and M.Pietikainen, “Video texture synthesis with Multi-frame LBP-TOP and diffeomorphic growth model”, 2013.
[3] R.J.Anderson and M.G.Kuhn, “Image retrieval with interactive query description and database revision”, 2012.
[4] B.Yang and T.Zeng, “Minimizing additive distortion in steganography using syndrome-trellis codes”, 2011.
[5] H.Otari and S.Kuriyama, “Texture synthesis for mobile data communication”, 2009.
[6] S.C.Liu and W.H.Tsai,”Line-based cubium-like image-A new type of art image and its application to lossless data hiding”,Oct. 2012
[7] Y.M.Cheng and C.M.Wang,”A high-capacity steganographic approach for 3D polygonal meshes”, vol. 22, 2006.
[8] C.Han, E.Risser, R.Ramamoorthi, and E.Grinspum, “Multiscale texture synthesis”, vol. 27, 2008.
[9] H.Otori and S.Kuriyama, ”Data-embedded texture synthesis”, 2007.
[10] K.Xu et al., “Feature-aligned shape Texturing”, vol. 28, 2009.