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: 6.199

IJCSMC, Vol. 9, Issue. 1, January 2020, pg.144 – 149

Hiding Data in Video Sequences using RC6 Algorithm

[1]V.Yamini Priya; [2]K.Priyadharshini; [2]K.Sowndharya; [2]S.Swathi; [2]K.Swetha

[1]Assistant Professor, Department of CSE, VSBCETC, Coimbatore, India

[2]UG Scholar, Department of CSE, VSBCETC, Coimbatore, India

Abstract— An enhancement of data protection system for secret data transmission using reserve room in encrypted images based on texture analysis with lifting wavelet technique is proposed here. The wavelet will split the image into four frequency sub bands namely LL, LH, HL and HH. These coefficients are then used in the encoder for removing the redundancies. The selective embedding is utilized in this method to find host signal samples suitable for data hiding technique. This method uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. The binary representation of the each hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. The Least significant bit replacement method is effectively used for data hiding process. This method proves as more secure technique for secret data transmission with high quality factor. The hidden data will be used to enable the receiver to reconstruct the same secret transformation table after encryption. Hence the original image can be reproduced by the inverse of the transformation and encryption processes. We proposed the encrypting user's data using RC6 Algorithm with a Secret Key, Which is embedded effectively in a Image using LSB based image steganography techniques. The simulation produces result to indicate that the framework can be successfully used in Image data hiding applications. This can be used for hiding data in video frames to avoid data to be attacked by attacks. Hence it is efficient and provides good accuracy.

Keywords— Steganography, Chaos algorithm, LSB technique, RC6 algorithm, LWT technique

INTRODUCTION

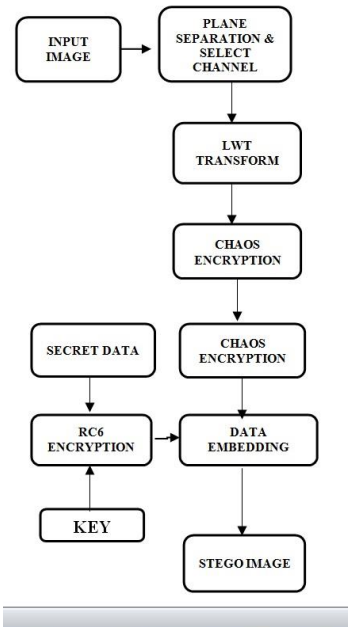
Image processing is a method to perform some operations on an image, in order to determine an enhanced image or to extract some useful information from it. Image processing is increasing now-a-days and it has different techniques included. Here we use a steganographic technique in Image processing. The word Steganography means "Hidden Writing". Some examples include, shaving scalp of a most trusted slave to etch a secret message and waiting for the hair to grow after which he was sent to another person who retrieves it by his head. Engraving messages on wooden Tablet and then covering it wax. The receiver retrieves the secret message by melting the coated wax. Steganographic process deals an art with technological revolution has now evolved into a science to avert detection of hidden data delivered terminology for steganography while Simmon gave the first model for steganography by

explaining the scenario of Alice and Bob held in separate prison cells had to communicate through Warden Wendy. Types of steganographic system includes pure private key and public key respectively, whereas three techniques for steganography including insertion, substitution and cover generation have been discussed . Cryptography, having origin and with same inception period as that of steganography, means "Secret Writing" the essence of which is to inarticulate secret information in contrast to steganography whose sole perseverance is to conceal the fact that such information does really exist. Nowadays secure transfer of private information is a major issue over the internet. Because now-a-days the whole communication is done through internet and transferring private data from one end to another using various applications such as e-mails, chats, etc. But there is main issue to protect our confidential information from hackers or cyber criminals over internet. To solve those problems and to maintain the security of data, we should follow a algorithm which should not only encrypt the data into another form but also hides its presence and video steganography helps to provide a secure environment over internet. To protect the private information from being misused by the unauthorised user and to overcome the alteration of information a novel data hiding approach is used. Here hides the presence of secret message behind a multimedia file without changing the perceptual quality of media file and provide secure communication between two persons. Steganography can be used as text, image, audio, video based and protocol based steganography. Here we are dealing with video steganography using RC6 algorithm. The process of hiding the secret information behind video bit streams is video steganography. The main goal of this project is to hide presence of secret message from human visual system. Various companies and organizations are following this concept to secure their confidential information and databases from attackers. Video files can hide large amount of hidden data behind their bit streams rather than images. So, that's why they are more preferable than image steganography.

PROPOSED SYSTEM

The proposed system ensures the data protection system for secret data transmission based on, Security Enhancement system through Video Encryption, Data encryption and adaptive data embedding technique based on Chaos encryption. Now this encrypted image and cover image are the inputs of the Stego System which uses LWT and a specific steganographic algorithm and outputs a Stego image. RC6 and adaptive LSB (least significant bit) replacement algorithm.

Block Diagram:



Steganography Process

Frame Separation: An Video(avi) files are converted into frames for processing it and detect the moving objects. These sequence of images gathered from video files by finding the information about it through 'video info' command. These frames are converted into images with help of the command 'frame2im'.Create the unique name to each frames and this process will be continued for all the video frames.

Encryption: In cryptography, encryption is the process of encoding messages that only authorized persons can read it. Encryption does not prevent interception, but also not to allow the message content to the interceptor. In an encryption scheme, the intended communication message, referred to as plaintext which is in human readable form, is encrypted using an encryption algorithm and generating corresponding cipher text which cannot read by humans. So it can only be read if decrypted.

Steganography: Steganography is the process of hiding a message within a larger one that someone cannot know the contents of the hidden information. Although related, Steganography is not to be confused with Encryption process, which is the process of making a message meaningless. Steganography tries to hide the existing of communication.

Lifting Wavelet Transformation:

LWT fragmented the image into different sub band images, namely, LL(low to low), LH(low to high), HL(high to low), and HH(high to high) for inserting the messages in the pixel coefficients of sub bands. LL (low to low) sub bands contains the important part of the spatial domain image. High-frequency sub band contains the edge information of input image.

Integer Wavelet Transform (IWT) can be obtained through lifting pattern. Lifting pattern is a technique to convert DWT (Discrete Wavelet Transform) coefficients to Integer coefficients without losing information. The secret text information is inserted into the wavelet coefficients of high frequency sub bands because it is insensitive to human visual system.

Methodologies:

- Plane Separation
- Chaos crypto system
- Lifting Wavelet Transform
- RC6 Encryption
- LSB Embedding and Extraction
- Performance analysis

DECOMPOSITION PROCESS:

The wavelet transform has obtained widespread acceptance in signal processing and image compression. LWT process transforms the spatial domain pixels into frequency domain information that are entitled in multiple sub-bands, representing different time scale and frequency points. In which image split into 4 level of sub bands they are low to low level, low to high level, high to low level, high to high level. These sub bands are represent pixel, edge, shape and texture of the image. It is 360 degree process

STEGNOGRAPHY USING LSB:

Maintaining the confidentiality of digital information when being communicated over the Internet is presently a problem, given the amount of cheap computation power available and certain known limitations of the encryption methods it is not too difficult to launch attacks on ciphertext. An ideal steganographic technique inserts message or information into a carrier image with virtually unnoticeable modification of the image. Adaptive Steganography comes closer to this ideal since it utilize the natural variations in the pixel intensities of a cover image to hide the secret information. The objective of steganography is a process of embedding an additional information into the digital contents that is invisible to listeners. We are look-over its embedding, detecting, and coding techniques. The scheme behind the LSB algorithm is to insert the bits of the hidden information into the least significant bits of the pixels. As the application domain of inserting data in digital multimedia sources becomes widen, several terms are used by various groups of researchers, encompasses with steganography, digital watermarking and data hiding. This paper explains a new, principled approach to finding least significant bit (LSB). Steganography in digital signals like images and audio. It is shown that the length of hidden messages inserted in the least significant bits of signal samples can be calculated with relatively high precision.

DATA ENCRYPRTION:

CHAOS ENCRYPTION:

This method is one of the advanced encryption standard to encrypt the text data for secure transmission. It encrypts the original text message with encryption key value generated from chaotic sequence with threshold function by bit xor operation Here logistic map is used for generation of chaotic map sequence. It is very useful to transmit the secret text data through unsecure channel securely which prevents data hacking. The chaotic system is defined on a complex or real number space called as boundary continuous space. Chaos' theory generally aims that to recognize the asymptotic action of the iterative progression. The properties essential for chaotic systems designed for cryptography is sensible to an initial condition with topology transitivity.

Optimum Pixel Adjustment Process:

The proposed Optimal Pixel adjustment Procedure (OPAP)decreases the error produce by the LSB substitution method. In OPAP scheme the pixel value is adjusted after the secret information is hidden. It is done to upgrade the quality of the stego image without disturbing the information hidden Adjustment Process.
Let ‘n’ LSBs be substituted in each pixel.
Let d= decimal value of the pixel after the substitution.

d1 = decimal value of last n bits of the pixel.
d2 = decimal value of n bits hidden in that pixel.
If(d1~d2)<=(2^n)/2
then no adjustment is made in that pixel.
Else
If(d1<d2)
d=d–2^n .
If(d1>d2)
d=d+2^n .

This d is converted to binary and written back to pixel.

EMBEDDING PROCESS:

In which data hide behind the cover image then we get stego image. Adaptive LSB technique will be used. In which data will be stored in least significant of each pixel value.

RC6 Algorithm:

RC6 is a securable, compact and simple block cipher algorithm. It offers good performance and considerable flexibility. Further it is simplicity, which will allow analysts to quickly refine and improve our estimates of its security. From the result analysis of all the phases discussed above sequential and sections phases gives the best and fastest execution time result of the Rivest Cipher 6 in an OpenMP.

Advantages:

- It avoids the leaks of video content in storage of clouds.
- Reduced time consumption process.
- It is useful to perceive video tampering.
- Better compatible system for people privacy protection

Application:

- Secret Data Communication in Defense.
- Research institute.
- Medical Information Protection
- Military Application.

CONCLUSION:

In this paper we gain a high security and accuracy can be achieved. A secret message can be hidden behind the frames of the video and it can be send from sender to receiver. Where the receiver can view the secret message by using the pass key. More security is achieved because the key can’t be identified by attackers.

REFERENCES

[1] Q. Kester, "A cryptographic Image Encryption technique based on the RGB PIXEL shuffling A cryptographic Image Encryption technique based on the RGB PIXEL shuffling", International Journal of Advanced Research in Computer Engineering & Technology, vol. 2,no.2 pp.848-854, January 2013.

[2] P. Sahute, S. Waghamare, S. Patil, and A. Diwate, " Secure Messaging Using Image Steganography", International Journal of Modern Trends in Engineering and Research,vol.2,no.3, pp. 598–608, March 2015.

[3] N. Agarwal and P. Agarwal, "An Efficient Shuffling Technique on RGB Pixels for Image Encryption", MIT International Journal of Computer Science & Information Technology, vol. 3, no. 2, pp. 77–81, August 2013.

[4] K. Hamdnaalla, A. Wahaballa, and O. Wahballa, "Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithms", International Journal of Video & Image Processing and Network Security, vol.13, no. 04,August 2013.

[5] N. G. A. P. H. Saptarini, Y. A. Sir, "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map", Information Systems International Conference, December, pp. 2–4, December 2013.

