Secret Data Sharing Through Video Using Adaptive Data Concealment With Crypto System

B.Prabhakaran, A.Murugan

Abstract: Nowadays, Internet and digital media are getting more popular. So, the need and requirement for secure transmission of data also increasing rapidly.A given input video file is converted into frame sequences and one of frame will be selected to conceal the secret data for secured data communication. The proposed technique uses chaos crypto system for encrypting a secret text data into cipher text to avoid data hacking issues. After data encryption, the data hider will conceal the secret encrypted data into the selected frame using adaptive embedding algorithm. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. These unnatural messages usually attract some unintended observers' attention. The data hiding technique uses the adaptive LSB replacement algorithm for concealing the secret message bits into the image in frequency domain. An Integer wavelet transform is used to determine the high frequency components for effective data concealing for preserving image quality. In the data extraction module, the secret data will be extracted by using relevant key for choosing the pixel coefficients and it will be decrypted to get original data using encryption key. Finally the data encryption and hiding will be analyzed based on image and data recovery.

Index Terms: chaos encryption, adaptive embedding algorithm, LSB replacement.

1 Introduction

Digital image processingperforms image processing on digital images with use of several algorithms. This process would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures.Image can be processed optically or digitally with a computer.To digitally process an image, it is first necessary to reduce the image to a series of numbers that can be manipulated by the computer. Each number representing the brightness value of the image at a particular location is called a picture element, or pixel. A typical digitized image may have 512 × 512 or roughly 250,000 pixels, although much larger images are becoming common. Once the image has been digitized, there are three basic operations that can be performed on it in the computer. For a point operation, a pixel value in the output image depends on a single pixel value in the input image. For local operations, several neighbouring pixels in the input image determine the value of an output image pixel. In a global operation, all of the input image pixels contribute to an output image pixel value. There are 3 types of images used in Digital Image Processing. They are

1. Binary Image
2. Gray Scale Image
3. Colour Image

1.1. Binary Image

A binary image is a digital image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white though any two colors can be used. The color used for the object(s) in the image is the foreground color while the rest of the image is the background color.

1.2. Gray Scale Image

A gray scale Image [5] is digital image is an image in which the value of each pixel is a single sample,that is, carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray(0-255), varying from black(0) at the weakest intensity to white(255) at the strongest.

1.3. Color Image

A (digital) color image is a digital image that includes color information for each pixel. Each pixel has a particular value which determines its appearing color. This value is qualified by three numbers giving the decomposition of the color in the three primary colors Red, Green and Blue. Any color visible to human eye can be represented this way. The decomposition of a color in the three primary colors is quantified by a number between 0 and 255. For example, white will be coded as R = 255, G = 255, B = 255; black will be known as (R,G,B) = (0,0,0); and say, bright pink will be : (255,0,255).

Cryptography

The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography; the "key" in this case being the knowledge of the method being employed (security through obscurity). Steganography [4] books are filled with examples of such methods used throughout history. Greek messengers had messages tattooed into their shave head, concealing the message when their hair finally grew back. Wax tables were scraped down to bare wood were a message was scratched. Once the tablets were rewaxed, the hidden message was secure [4]. Over time these primitive cryptographic techniques improved, increasing speed, capacity and security of the transmitted message.

Steganaography

Steganography [4] means to hide secret information into innocent data. Digital images are ideal for hiding secret information. An image containing a secret message is called a cover image. First, the difference of the cover image and the stego image should be visually unnoticeable. The embedding itself should draw no extra attention to the stego image so that no hackers would try to extract the hidden message illegally. Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if

- *B.Prabhakaran , is currently pursuing masters degree program in Computer Science and engineering in SRM University, India, PH-+91 9789505848. E-mail: mailme2prabha@gmail.com*
- *A.Murugan,Asst professor, Department of Computer Science and Engineering,SRMUniversity,India.PH-+91 9677066686. E-mail: murugan.abap@gmail.com*

she/he does not have a special extracting method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible.

CRYPTOGRAPHY VS STEGANOGRAPHY

Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary after the information is hidden. Information to be hidden + cover object = stego object. Information to be hidden + cover object = stego object. To add more security the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have the key. A stego object is one, which looks exactly same as cover object with an hidden information.

2 PROPOSED WORK

The proposed architecture consists of Data Protection system for secret data transmission based on, Security Enhancement system through Data encryption and adaptive data embedding technique based on chaos encryption and adaptive least significant bit replacement algorithm. The proposed sytem architecture diagram is shown below

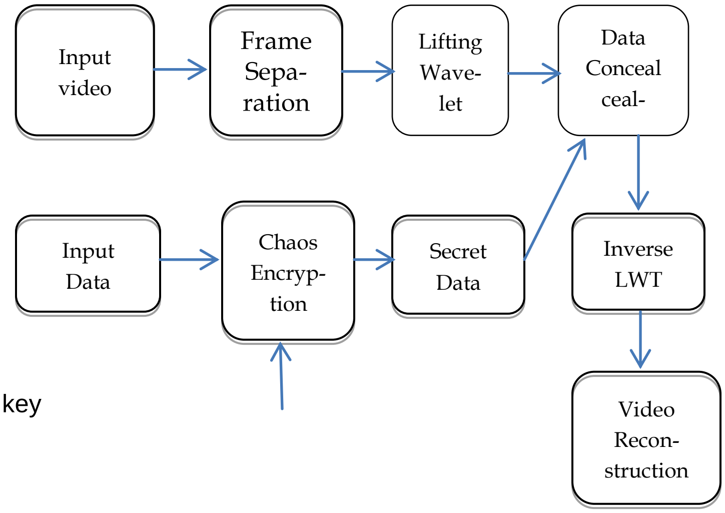

***Fig a)** proposed architecture diagram for data embedding*

Given input video is separated into several frames.Lifting wavelet is applied to find the high frequency region to conceal the data.Secret data can be encrypted using chaos encryption and embedded in the Video using Adaptive LSB replacement algorithm.Video can be reconstructed finally and stego video is obtained.

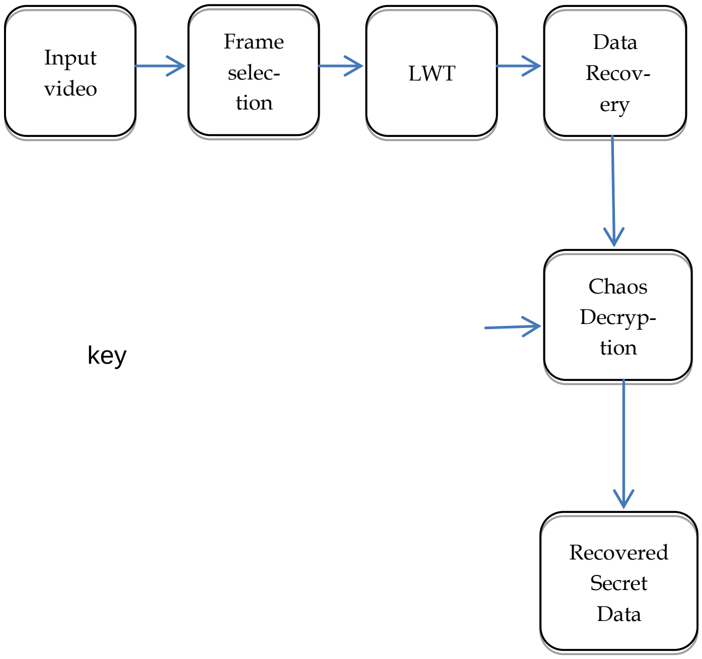

***Fig b)** proposed architecture diagram for data Extraction*

In the Extraction part the stego video is taken as input and the election of frame is done to extract the data.Decrypting the data using the relevant key to obtain the secret data in the plain text format.

FRAME SEPARATION

An Input Video(.avi files) are converted into still images. The sequence of frames are gathered from video files by using 'avi info' command. These frames are converted into images with help of the command 'frame2im'.This process will be continued for all the video frames.

LIFTING WAVELET TRANSFORM

LWT decomposes the image into different subband images, namely, Low-frequency and High frequency for embedding the messages in the pixel coefficients of sub bands. Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information. The secret text data is embedded into the wavelet coefficients of high frequency sub bands because it is non-sensitive to human visual system.

CHAOS ENCRYPTION

This method is one of the advanced encryption standard to encrypt the secret text data for secure transmission. It encrypts the text data's with encryption key value generated from chaotic sequence with threshold function by bitxor operation .It is very useful to transmit the secret data through unsecure channel securely which prevents data hacking.

LSB EMBEDDING

A 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant Stego-image which holds the secret message is also a 8-bit gray scale image. Difference between the cover image and the Stegano-image is not visually perceptible.

DATA EXTRACTION

The secret data can be extracted from the embedded video with help of key matrix and same frame used at embedding. This extraction process is opposite to data embedding. Finally, Extracted cipher text data will be decrypted using chaos decryption with encrypted key which is used at embedding stage.

3 SYSTEM REQIREMENTS

The software required is MATLAB 7.5 and above versions. The hardware required for the experiment is Intel processor with RAM capacity of 1GB. Hard disk capacity is 250 GB.

4 CONCLUSION

In this approach finally we can achieve a secured way for transmission of data through media(video).It provides high embedding capacity without degrading the image quality. It is efficient than the previous method. Data can be received efficiently without any loss on the receiver side. Secret data can be encrypted from plain text to cipher text and embedded in the video. The receiver should extract the video and decrypted the data from cipher text to plain text using relevant key.

REFERENCES

[1]. C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, “Adaptive data hiding in edge areas of images with spatial LSB domain systems,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[2]. F. C. A. Fernandes, R. L. C. van Spaendonck, and C. S. Burrus, “A new framework for complex wavelet transforms,” IEEE Trans. Signal Process., vol. 51, no. 7, pp.1825–1837, Jul. 2003.

[3]. T. Wiegand, G. J. Sullivan, G. Bjntegaard, and A. Luthra, “A Feasible Chaotic Encryption Scheme for Image,” IEEE Trans.., vol. 13, no. 7, pp. 557–559, Jul. 2003.

[4]. T Mrkel,JHPEloff and MS Olivier .”An Overview of Image Steganography,” in proceedings of the fifth annual Information Security South Africa Conference ,2005.

[5]. Souvik Bhattacharyya, Avinash Prasad Kshitij, Gautom-Sanyal, “A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform.,” 2010 International Conference on Recent Trends in Information, Telecommunication and Computing.

[6]. C. S. Burrus, R. A. Gopinath, and H. Guo, Introduction to Waveletsand the Wavelet Transform—A Primer. Englewood Cliffs, NJ: Prentice-Hall, 1998, Expansion of notes for the IEEE Signal Processing Society’stutorial program held in conjunction with the ICASSP-93 on Apr.26, 1993.