ISSN 23499842(Online), Volume 2, issue 1 March 2017
International Journal of Innovative Trends and Emerging Technologies

ENCRYPTED DATA HIDE IN COMPRESSED VIDEO USING SECURITY ANALYSIS

S.Sivasakthi1, G.Laxmanaa*
[1]*UG Student, Department of ECE,Agni college of Technology,Thalambur,Chennai*
[*]*Corresponding author:Assistant professor,Department of ECE ,Agni college of Technology,Thalambur,Chennai*

Abstract
Data hiding approach is necessary to perform in these encrypted videos for the purpose of content notation and tempering detection in this way, data hiding in encrypted domain without decryption preserves the confidently of the content in addition ,it is more efficient without decryption followed by data hiding and re-encryption. a data hider man embedded additional data in the encrypted domain by using bits replacement technique, without knowing the original video content. the project simulated results shows that used methods provides better performance interms of computation efficiency,high data security and video quality after decryption. The parameters such as mean square error, psnr, correalation are evaluated to measure its efficiency.

Index terms: Encryption, Decryption, data hiding, PSNR, MSE

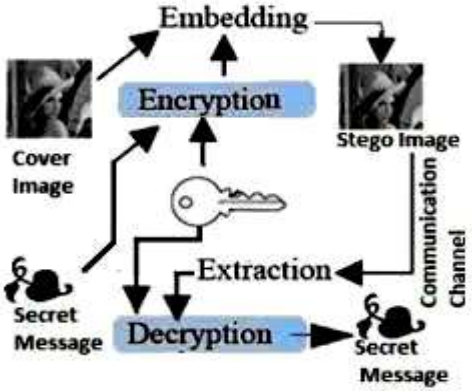
1. Introduction
Data hiding and watermarking in digital images and raw video have wide literature.this paper targets the internal dynamics of the video compression specifically the motion estimation stage.[1][2] we have chosen this stage because its contents are processed internally during ,the video encoding ,decoding ,which makes it hard to be detected by image stegno-analysis methods and is lossless coded, thus it is not prone to quantization distortions. data hiding in motion vectors relies on changing the motion vector based on their attributes such as their magnitude ,phase angle, etc. the data of bits of the message are hidden in some of the motion vectors whose magnitude is above a predefined threshold are called candidate motion vectors .

The following data hiding in compressed video. The input video is separated into frames . then he frames are subjected to dct and human coding to compress the frame [3].using the secret key .the steganography has been used for long time before .the main use for it was military and government messages. The approaches of steganography become widely used for many purpose [4].the researches provide and found out many approaches while others enhanced the existent methods.

Reversible data hiding is a technique in image processing area for encryption, by which the original cover can be losslessly recovered after the embedded message is extracted. selective encryption is a new trend in image and video content protection .it consists of encrypting only a subset of the data .the aim of selective encryption is to reduce the amount of the data encrypt while preserving, a sufficient level of security.

2. Working
Select the image that could be encode the secrete data.encode the data into the color image of the pixels are select from alternate location of pair of text.image having details about pair of text the image is encoded in each color frames R,G and B respectively[2][3]. Encode the text as a bit of color image the image consist of secret data embedding in the select image. the original image can be overwrite the secret image to increase the transferring rate of image the data can be compressed after embedding the data the encrypted key can be used to secure data.the secret data recover from the encoded color image encoded color image which has the information of secret text[3][6].The LSB bit of color image has '1' or '0' the resulted encoded text which has the pixels of that image .the recovery of secret data can be drawn from the original image the secret data can be viewed by the receiver.

3. Steganography
Steganography is the process hiding a secret message within a larger one in such way that someone cannot know the presence contents of the hidden message. Steganography includes the concealment of information within computer files. in digital steganography, communication may include steganography coding inside of a transport layer such as a document file program[5][6]. Media files for steganography transmission because of their larger size. as a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphet,a change so much so suitable that someone not specifically looking for it is unlikely to notice it.



Figure(a) steganography

4.Cryptography
The word cryptography comes from the greek words hidden and secret and writing .oddly enough ,cryptography is the art of the secret writing .more generally, people think of cryptography is the art of mangling information into apparent unintelligibility in a manner allowing secret method of untangling. in this book we will concentrate on the kind of cryptography that is based on representing information as numbers and mathematically manipulating those numbers.[3][6] This kind of cryptography can provide other services ,such as integrity checking reassuring the recipient of a message has not been altered since it was generated by a

legitimate source authentication verify some one identify but back to the traditional use of cryptography.

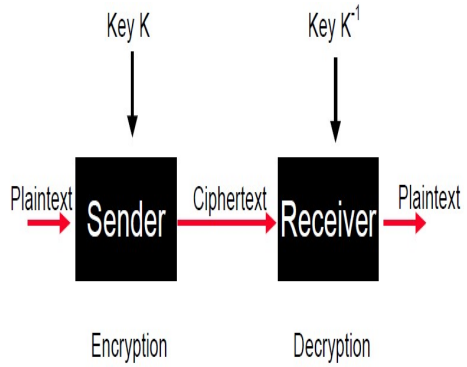


Figure (b) cryptography

In the novel approach of hiding image in video the proposed algorithm is replacing one replacing one lsb of each pixel in video frame it becomes very difficult for intruder to guess that an image is hidden in the video as individual frame are difficult to analize the video running at30 frame per second and we seen that only one LSB substation are used ;.[6] Another work on this topic has been presented bymargin Mohamed and Mohamed benata"D ata hiding by LSB substitution using generic optimal key permutation.

5. DATA HIDING

A security product based on an unrivalled data hiding method .as a result of many months of research, this product hides safely protects your private information from being erased.3][5] Would you be happy to find your priceless financial plans, your personal ideas or project,

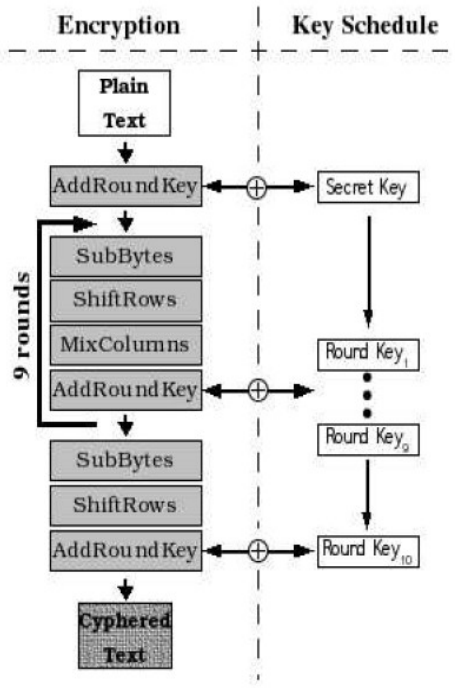


Figure (c) Data hiding

your private photos or movies n foreign hands, altered or erased .hide secret files is the ultimate tool allowing you to have exclusive secured access to sensitive information based on a password .no one except you, who know the password, will be able to access the secured data .not even your own operating system will have permission to alter the information. The latest, and one of the most annoying secondary products of the internet evolution, is the spy-ware activity. And thankfully t is absolutely in offensive against the protection guaranteed by hide secret files[4]. The hidden data won not be visible even for your own, so the safe mode booting or moving the hard drive.

6. Methodologies:

An Efficient data hiding approach on encrypted compressed video bit streams for privacy information protection based on. A input video or audio /video input is a port network jack is what receivers a signal video from one device to another or video output source. one of the most common video input cables is the composite[1][4] .An input video are converted into still images for processing it and detect the moving objects. These sequence of images gathered from video files by finding the information about it through "aviinfo" command. These frames are converted into images with help of the command "frame2im".H.264 or MPEG-4 part 10 ,Advanced video coding (MPEG-4 AVC)is a block-oriented motion compression based video compression standard. As of 2014 it is one of the most commonly used formats for the recording compression and distribution of video content. The application of the mathematical chaos theory to the practice of the cryptography, the study or techniques used to privately and securely transmitting formation with the presence of a third party or adversary. The least significant bit is the bit position in a binary integer giving the units value that is determination whether the number is even or odd. The LSB is sometimes referred to as the right most bit due to as the right most but due to the convention in positional notation of writing less significant digits further to the right. The mean squared error or mean square deviation of an estimator measures the average of the squares of the errors or deviations that is the difference between the estimator and what is estimated MSE is a risk function.

7.Result And Discussion

The Quality of the reconstructed image is measured interms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2.. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE} = \sigma_q^2 = \frac{1}{N} \sum_{j,k} (f[j,k] - g[j,k])^2$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10\left(\frac{255^2}{MSE}\right) \log_{10}$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

References

[1]W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.
[2] B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010.
[3] P. J. Zheng and J. W. Huang, "Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking, "in Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012, pp. 1–15.
[4] W. Puech, M. Chaumon and O. Strauss, "A reversible data hiding method for encrypted images," Proc. SPIE, vol. 6819, pp. 68191E-1–68191E-9, Jan. 2008.
[5] X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett. vol. 18, no. 4, pp. 255–258, Apr. 2011.
[6] W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process.199–202, Apr. 2012.
.