International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 07, July-2015

Region Incrementing Visual Cryptography Using Lazy Wavelet Transform

Ashlin Jose
Computer Science and Engineering
Adi Shankara Institute of Engineering & Technology
Kalady, India

Divya G
Computer Science and Engineering
Adi Shankara Institute of Engineering & Technology
Kalady, India

***Abstract*—Video steganography is the most widely used form of steganography. Steganography is an art of hiding the secret information inside digitally covered information. The hidden message can be text, image, speech or video and accordingly the cover can be chosen from either an image or a video. Here we perform steganography on videos and hide message in encrypted form, by this security is increased by two times. The message which is used here is shares which are produced by using region incrementing visual cryptography. The mostly used technique for hiding information in steganography is LSB (Least Significant Bit) steganography. But instead of simple LSB technique, here we will use Lazy Lifting Wavelet transform and then apply LSB in the subbands of the video that has been obtained. The proposed approach will utilize the video as well as audio component to hide message, in video component we will hide the encrypted message and in audio we hide the length, up to which the message is hide in video, using LSB technique.So here we can improve the security of region incrementing visual cryptography by using this technique.**

Keywords—Sub bands;LSB; Lazy wavelet;Region incrementing visual cryptography

I. INTRODUCTION

In today's era the challenge is to send and display the hidden information specially in public places. The reason is that intruders get information from a system is in a form that they can read and understand it. Intruders may modify it to misrepresent an individual or any organization, reveal the information to others, or use it to launch an attack. We can solve this problem by using steganography. Steganography is the process of hiding secret information in the form of cover which can be any multimedia file like image, audio, video, by which third party cannot recognizes that message which is existed . In steganography steganos means covered and graphie means writing. So simply means covered writing. The goal of visual cryptography is to protect the content of messages. Steganography is little bit contrast to visual cryptography. In steganography existence of the message will be hidden but in visual cryptography, is a cryptographic technique in which decryption can be performed without the use of computer.

The main difference between the steganography and the visual cryptography is that steganography involves hiding information so it appears that no information is hidden at all.If the object is viewed by person to know whether there is something hidden in it or not, then he or she will get no idea that there is any information which is written, so the person will not try to decrypt the information.

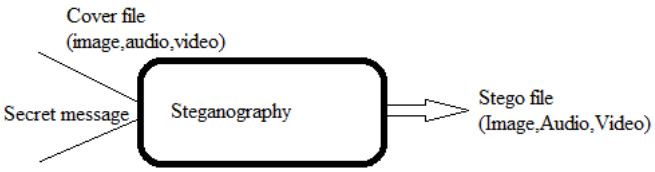


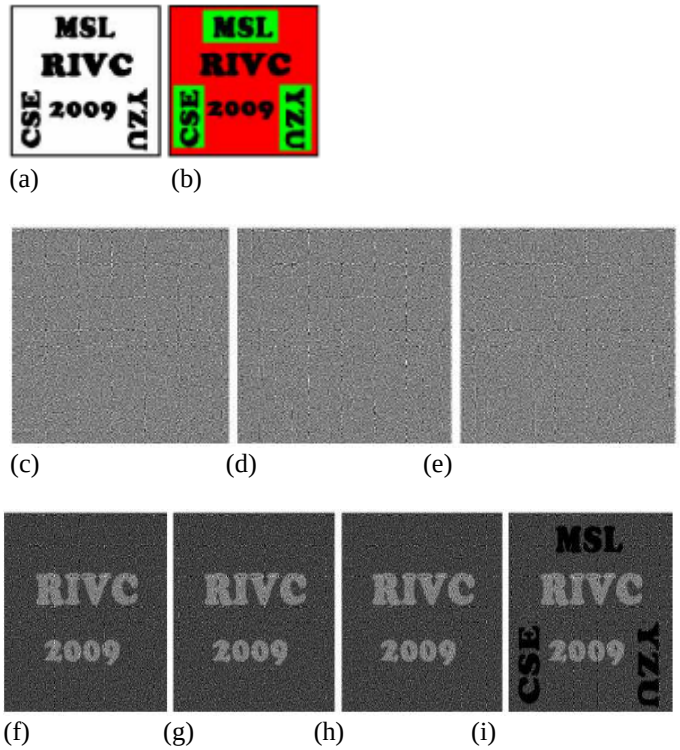
Fig.1.Basic Steganography System

Multimedia files, such as video, audio and images are generally use today. Images are good medium for hiding the data.. The more detailed the image, the lesser constraints there are on how much data it can hold without it becoming noticeable. For hiding data in audio files, there are many tools available for it. The large size of audio files made it less popular than image files as a medium for steganography. When compared with video both images and audio have less storage capacity. There are many visual cryptography algorithms have been created which turn the data into shares.. Visual Cryptography is a secret-sharing method which encrypts a secret image into several shares but it doesnot require any computer calculation to decrypt the secret. Visual cryptography was introduced by Naor and Shamir.Here firstly we divide the original image into encrypted form which is known as shares or shadows then we can reconstruct the original image by superimposing these shares.

II. RELATED WORK

Steganography in video is done by applying transformation techniques. This can be achieve either in spatial domain or in frequency domain. In spatial domain the computation is done on pixel value directly while in frequency domain, firstly it is converted into frequency domain and then computation is done. There are many LSB techniques by which data can be encoded in image or video or any multimedia file. Depending upon the size of the cover and technique use the amount of data can be hidden. Before hiding the data, it can be secured by applying some visual cryptography technique which will convert the images into shares or shadows. After that reconstruction is taking place.

In this paper [2] sharing visual secrets with multiple secrecy levels in a single image is discussed . Firstly (2, n) region incrementing Visual Cryptography was introduced by Wang, here a secret image is divided into multiple regions. By stacking any t ($2 \leq t \leq n$) shares, up to ($t-1$) regions of the secret are visually revealed. The region incrementing property enriches some feasible applications of Visual Cryptography schemes. Later, Yang et al. proposed a k-out-of-n Region incrementing visual cryptography for providing flexible sharing strategy. However, the mentioned methods l suffer from pixel expansion and code book needed problems seriously. In essence, the regions in the secret image are revealed according to the quantity of stacked shares for the mentioned methods .



(a) (b) (c) (d) (e) (f) (g) (h) (i)

Fig.2. Basic Region Incrementing visual cryptography

(a) Secret image (b) secrecy-level decomposition (c)-(e) Three encoded shares
(f)-(h) superimposing any two of the three shares (i) superimposing all three shares

Adaptive Region Incrementing XOR based Visual Cryptography

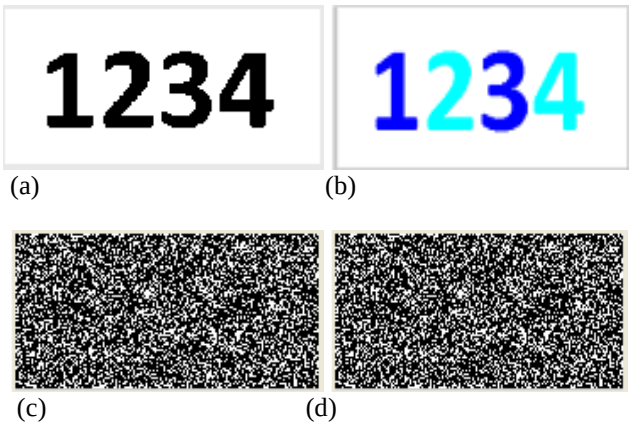
In this paper [1] XOR based visual cryptography with adaptive security level is used which is known as adaptive region incrementing XOR based visual cryptography. Here security levels are assigned by using security level assignment algorithm.This algorithm mainly based on the concept of general access structure.The operation which is used for the reconstruction is XOR. Let p = {1,….n) be a set of elements called participants of a visual cryptography and let 2p denote the set of all subsets of p. Let rqual $\subseteq$ 2p and rforb $\subseteq$ 2p. rqual $\cap$ rforb= $\emptyset$. Members of Γqual are defined as qualified sets and members of Γforb are defined as forbidden sets.
The pair (Γqual, Γforb) is called the access structure of this scheme . Define Γ0 consist of all the minimal qualified sets

Algorithm

Input: A binary secret image M with background L0 and k security levels L1, . . . , Lk , and an access structure (rQual, rForb) whose minimal qualified sets are with initial security levels.
Output: n shares R1, . . . , Rn.
1) Assign initial security level to minimal qualified sets in r0
2)The remaining qualified sets which are not assigned the initial security level are automatically given by using the security level assignment algorithm.
3)After this share generation begins.

Algorithm mainly consists of two components
1)The generation of p pixels and
2)The construction of the remaining n −p pixels.
For each time, a pixel m is constructed based on the security level of given secret pixel.
A qualified setwhich contains p participants, is randomly chosen from the basis. According to the selected minimal qualified set, p−1 shared pixels are randomly generated, and the shared pixel is constructed in accordance with p−1 random pixels and the secret pixel using XOR operation. For the remaining n−p shared pixels, they are generated iteratively based on the secret pixel and the former shared pixels that have been assigned values.

Security Level Assignment.
Input: An access structure (rqual, rforb) whose minimal qualified sets are with initial security levels.
Output: Qualified sets in rqual with assigned security levels.
Consider, a sharing strategy with three participants {1, 2, 3}and a three security level secret image is considered.
Let r0 = {{1, 2}, {1, 3}} and rqual = {{1, 2}, {1, 3}, {1, 2, 3}}.
We assign the initial security level L1 to {1, 2} and assign L2 to {1, 3}. Then, the algorithm completes the security level assignment for qualified set {1, 2, 3}.. Therefore, the security level of {1, 2, 3} is L3.



(a) (b) (c) (d)

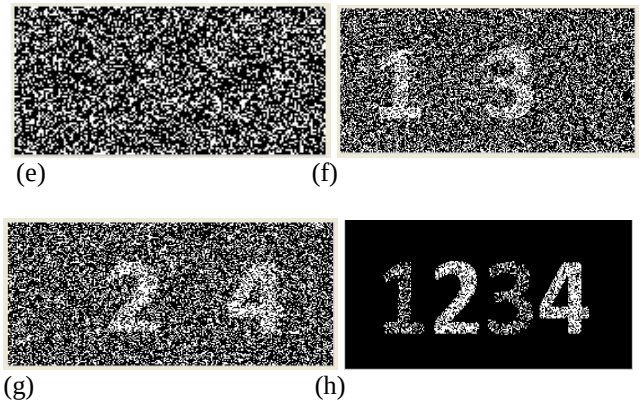


Fig.3. Experiment by the adaptive region incrementing XOR based visual cryptography with 2 security levels. (a) Secret image with 2 security levels (b) figure defining region (c)-(e) Three shares R1,R2,R3 (f) R1 XOR R2 (g) R2 XOR R3 (h)R1 XOR R2 XOR R3.

III. PROPOSED TECHNIQUE

A. Visual Cryptography Model

In this model we will use the Adaptive region incrementing XOR based visual cryptography algorithm, which will convert the image into shares, which provide a high security. And this data is stored in frames of Video after that video can be send. At the receiving side, the shares are retrieved and converted to original image by stacking them together.

B.Hiding Procedure

A video is consisted of multiple frames. We will use some frames of video in sequential order, and each frame (image) is treated as unique image and is use to store shares. A steganography technique is use to store share here we use the 2D - Lazy Wavelet Transform on each frame to get four sub-bands. The data is then hidden in subbands of frames using LSB technique. The length of data which is stored in frames is hide in audio using simple LSB technique.

C.Applying Lazy Wavelet Transform on the Frames of the Video

A video is comprised of many frames. On each frame we apply a image transformation technique. Wavelet transformation is use to convert the spatial domain into frequency domain but most of the wavelet techniques produce real values, which will result in data loss when is hide and retrieved. So to overcome this we use lazy wavelet scheme, by applying Integer Wavelet Transform which produces integer values. After applying Integer Wavelet Transform we get four subbands.

D. Hiding bits in the Four Sub-bands

Using LSB technique we can hide shares in sub bands.After the shares are retrived we can reconstruct the original image by stacking them together

IV. ALGORITHM FOR IMAGE HIDING

Step 1: Extract all frames from video
Step 2: Select 1st Frame I from Video
Step 3: Apply Lazy wavelet scheme to produce 4 subbands (cA cH cV cD).
Step 4: Hide shares on these sub bands
Step 5: Transmit video through secure channel

V. ALGORITHM FOR IMAGE RETRIEVAL

Step 1: Extract all frames from video
Step 2: Select 1st Frame I from Video
Step 3: Apply Lazy wavelet scheme to produce 4 sub bands (cA cH cV cD).
Step 4: Apply Region Incrementing Technique to reconstruct the original image.

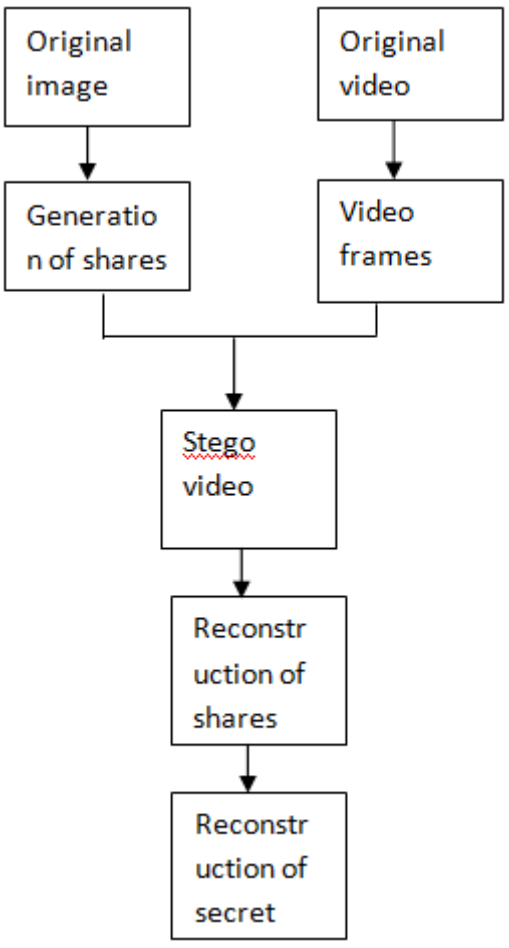


Fig.4. Flowchart representing the proposed technique

VI . CONCLUSION

Steganography is the art of hiding information in digital media in order to conceal the existence of the information. This paper provides a good method of steganography in video by using adaptive region incrementing XOR based visual cryptography algorithm. Lazy Wavelet Scheme and LSB technique.are mainly used here. The data is hidden in video and the length is hidden in audio component using LSB technique, and the changes which are done in both the components is not recognizable. The proposed technique provides two layer securities by visual cryptography and Steganography. The technique provides a good capacity to store a high load message.The proposed technique can be use in copyright control of materials, medical records, TV broadcasting, financial companies data safe circulation, smart Id cards and banking.

REFERENCES

[1] Xiaotian Wu and Wei Sun," Extended Capabilities for XOR-Based Visual Cryptography*" IEEE Transactions On Information Forensics And Security, Vol. 9*, No. 10, OCTOBER 2014

[2] R.-Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Process. Letter.*, vol. 16, no. 8, pp. 659–662, Aug. 2009.

[3] D. Artz, "Digital Steganography: Hiding Data within Data,*" IEEE* Internet Computing Journal, June 2001.

[4] Ming Chen, "Analysis of Current Steganography Tools:Classifications & Features," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006*, pp. 384 – 387, 2006

[5] Dipti Kapoor Sarmah and Neha Bajpai, "A new horizon in data security by Cryptography & Steganography,*" International Journal of Computer Science and Information Technologies*, vol. 1, no. 4, pp. 212-220, 2010

[6] K. Gopalan, "Audio steganography using bit modification," *In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03)*, pp. 421-424, 2003.

[7] Krishna Bhowal, Anindya Jyoti Pal, G.S. Tomar & P.P. Sarkar, "Audio Steganography using GA", IEEE International Conference on Computational Intelligence and Communication Networks CICN 2010, pp 449-453, Nov 2010

[8] W. Sweldens, "The lifting scheme: A construction of second generation wavelets," *SIAM J. Math. Anal.*, vol. 29, no. 2, pp. 511-546, 1997.

[9] G. Uytterhoeven, D. Roose, and A. Bultheel, "Integer wavelet transforms using the lifting scheme," in *Proc. Of the 3rd World Multiconference on Circuits, Systems, Communications and Computers*, Athens, pp. 6251-6253, 1999.

[10] M. F. Tolba, M. A. Ghonemy, I. A. Taha, and A. S. Khalifa, Using integer wavelet transforms in colored image steganography," *IJICIS*, vol. 4, no. 2, pp. 75-87, 2004.