Digital Secret Sharing using XOR based region incrementing and lazy wavelet in video

Ashlin Jose
Computer Science and Engineering
AdiShankara Institute of Engineering and Technology
Kalady, India

Divya G
Computer Science and Engineering
AdiShankara Institute of Engineering and Technology
Kalady, India

Abstract- Secret sharing is the process of distributing a secret amongst a group of participants each of whom is allocated a share of the secret. This secret can be reconstructed only when a enough number of possibly different types of shares are combined together. Individual shares have no use here Steganography can applied on video files and hide the message in an encrypted format thus achieving a multiple cryptographic system. The most frequently used technique is Least Significant Bit steganography (LSB steganography). But instead of traditional LSB encoding a modified encoding technique which will first transform the video using a Lazy Lifting Wavelet transform and after that apply LSB in the sub-bands of the video that has been obtained.

Index Terms- Region Incrementing Visual Cryptography; Video steganography;

I. INTRODUCTION

In today's era the challenge [1] 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 difficulty by using steganography. Steganography is the method 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 diference 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.

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.

Multimedia steganography is one of the most recent and secure forms of steganography. Visual steganography is the most widely practiced form of steganography. It started with concealing messages within the lowest bits of noisy images or sound files. We shall perform steganography on video files and hide the message in an encrypted format, thus achieving a multiple cryptographic system. The most commonly used technique is Least Signi_cant Bit steganography (LSB steganography). But instead of traditional LSB encoding, use a modified encoding technique which will firsts transform the video using a Lazy Lifting Wavelet transform and then apply LSB in the subbands of the video that we have gotten.

II. RELATED WORKS

A.Visual Cryptography

Visual cryptography is a special encryption technique for hiding information in images I.t can be decrypted by using the human vision if the correct key image is used.This method was proposed by Moni Naor and Shamir in 1994 . The original image is divided into 2 shares. Each pixel in original image is represented by non-overlapping block of 2 or 4 sub-pixels in each share. Anyone, having only one share cannot reveal any secret information. Both the shares are required to be superimposed to expose the secret image . In (2,2) Visual Cryptography Scheme, original secret image is divided into two shares. Each pixel in original image is represented by non-overlapping block of 2 or 4 sub-pixels in each share. Anyone having only one share can not reveal any secret information. Both the shares are essential for the superimposition and revealing of secret image .

B.k out of n visual cryptography scheme

In this k out of n visual cryptography scheme firstly the secret image is separated into n shares by performing some complex computations. In the decryption side only k or more number of shares can expose the original information and so less than k number of shares can not reveal the original secret.Major drawback of this scheme is pixel expansion and low contrast.

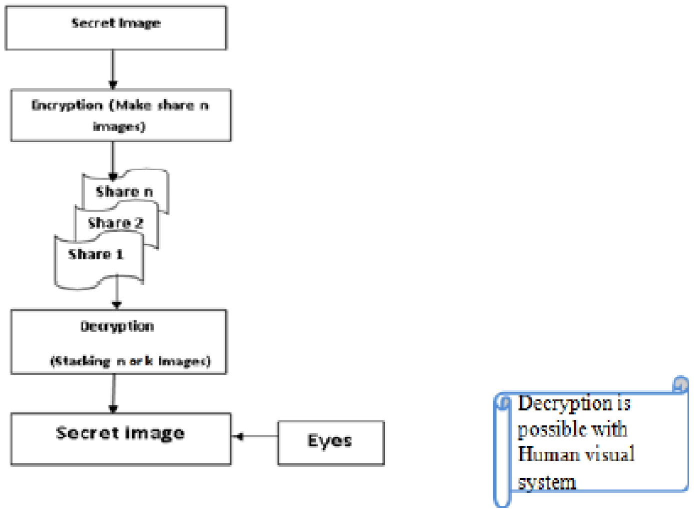

Fig 1: Visual Cryptography: Flow chart

C.Extended Visual Cryptography

One of the speciality of this scheme is that the shares which generated are meaningful in nature.Which allows the construction of visual secret sharing schemes .After the stacking of these shares this meaningful information will disappears and the secret is recovered. Meaningful shares avoid attention of hacker considering the security issues over the communication channels.

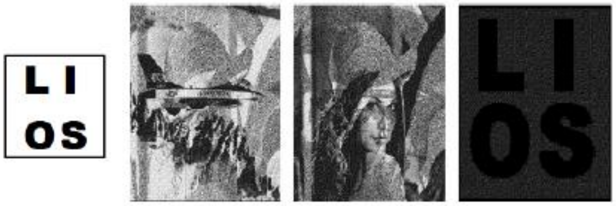

Fig 2:Extended visual cryptography

D.Halftone Visual Cryptography

Here encodes a secret binary image into n shares of random binary patterns.If the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies but no secret information can be revealed from the superposition of a forbidden subset.This type of visual cryptography scheme is better than extended visual cryptography scheme.But pixel expansion is also a major problem here.But it offers good contrast and security.

E.Visual Cryptography Scheme for General Access Structure

In (k, n) Visual cryptography scheme all n shares are in equal importance . Any k out of n shares can be able to reconstruct the original information. It may destroy the security of the system. To solve this problem G. Ateniese , C. Blundo , A. DeSantis , and D. R. Stinson extended (k,n) visual cryptography model to general access structure.In general access structurescheme set of n shares is divided into two subsets namely quali_ed subset and forbidden subset of shares as per the importance of shares. Any k shares from quali_ed subset of shares can reveal secret information, but less than k shares from quali_ed subset of shares can not reveal any secret information.This technique is applicable not only to the extended visual cryptography scheme but also to the conventional visual cryptography scheme.No code book is needed here.But this is not secure in nature.

Region Incrementing Visual Cryptography

In traditional visual cryptography scheme the whole image is considered as a single secret and same encoding rule is applied for all pixels of one image. So it reveals either entire image or nothing. It may be the situation that different regions in one image can have different secrecy levels, so we cant apply same encoding rule to all pixels. Ran-Zan Wang developed a scheme Region Incrementing Visual cryptography for sharing visual secrets of multiple secrecy level in a single image . In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions.

Efficient Construction for Region Incrementing Visual Cryptography

The important technique which is used here is linear programming [6].Which is used for the minimization of pixel expansion.High contrast is one of the important advantage of this scheme disadvantages are color reversal and pixel expansion problem.

k Out of n Region Incrementing Scheme in Visual Cryptography

Here k and n are integers that are able to reveal correct color of all regions [7].Incorrect color problem is solved here .And it theoretically satisfy both contrast and security conditions.This scheme is mainly solves the problem of wang's method that is incorrect color problem.

An Extended Region Incrementing Visual Cryptography Scheme Using Unexpanded Meaningful Shares

Region Incrementing is an active and important research area. In (2, n) region incrementing visual cryptographic scheme a single secret image is divided into multiple secret regions.Atleast 2 secret shares are needed to reveal the first region . After stacking more and more shares entire image is revealed.Color reversal,pixel expansion and low contrast are solved in thi technique.

Video Steganography and Wavelet Transform

Steganography

Steganography is the art and science of writing covert messages such that the presence of message is only known to both sender and recipient.This word is derived from greek words steganos means covered or protecting. Graphia means writing. Steganography mechanism is used to hide data like secret images and any other files within another file. Steganography and the cryptography mechanisms are combined together to send a secret data with full security. The best steganographic method that works in this domain is the LSB (Least Significant Bits) which replaces the least signi_cant bits of pixels selected to hide the information. There are four ways to implement steganography: 1. Using text. 2. Using images. 3. Using audio files. 4. Using video files.

Text Steganography
The medium which is used for hiding information is text. Text steganography can be classified mainly three basic categories 1) format-based 2)random and statistical generation and linguistic method.

Image Steganography
The most widely used technique is image steganography.This steganography technique exploits the weakness of the human visual system (HVS).The medium which is used for hiding information is image.

Audio Steganography
Here the medium which is used here is audio.In audio steganography secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file.

Video Steganography
Video files are generally a collection of images and sounds. so most of the presented techniques on images and audio can be applied to video files too. When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method. DCT works by slightly changing each of the images in the video, only so much that it is not noticeable by the human eye.

Wavelet Transform
As a mathematical tool wavelets can be used to extract information from many different kinds of data but certainly not limited to audio signals and images. Sets of wavelets are generally needed to analyze data fully. A set of complementary wavelets will decompose data without gaps or overlap so that the decomposition process is mathematically reversible. Thus sets of complementary wavelets are useful in wavelet based compression/decompression algorithms where it is desirable to recover the original information with minimal loss.

III. METHODOLOGY

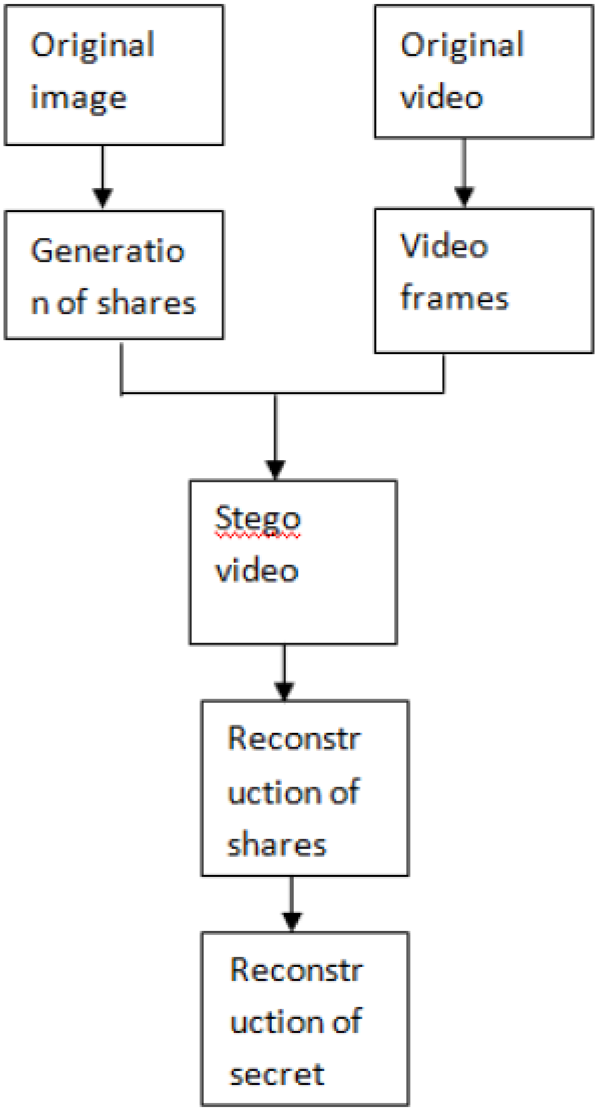

Fig 3:Proposed System

In this system firrstly we encrypt the message using the algorithm of adaptive region incrementing XOR based visual cryptography and after that hide the data into a video file that means we hide the data by using the frames of the video.This video will act like the cover.Each frame can be considered as different image and an image steganography method is applied here.So we use 2D lazy wavelet transform on each frame to get sub bands.The data is hidden in these four sub bands using LSB technique.The process of extracting the secret data from the steganographed video is just the reverse process of hiding the data in the video.

Adaptive Region Incrementing Visual Cryptography Using Lazy Wavelet Transform

Visual Cryptography Model

In this model we will use the Adaptive region incrementing XOR based visualcryptography 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.

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 subbands. 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.

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.

Hiding data in the Four Sub-bands

Using LSB technique we can hide shares in sub bands.After getting the subbands hide the message in the least significant bits (LSB) of the transform coefficients. The process of extracting the secret data from the steganographed video is just the reverse process of hiding the data in the video.

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 securre channel.

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

Adaptive region incrementing XOR based visual cryptography Algorithm

Input: A binary secret image M with background L0 and k security levels L1,. . . , Lk , and an access structure (quali_ed set,forbidden set) whose minimal qualified sets are with initial security levels.
Output: n shares R1, . . . , Rn. 1)
Assign initial security level to minimal qualified sets 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 set which 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 Algorithm

Input: An access structure (Quali_ed set,forbidden set) whose minimal qualified sets are with initial security levels.
Output: Quali_ed sets with assigned security levels. Consider, a sharing strategy with three participants 1, 2, 3and a three security level secret image is considered.

IV.EXPERIMENTAL RESULT

Adaptive Region Incrementing XOR Based Visual Cryptography by using lazy wavelet transform

Result analysis

MSE	PSNR	MD
301.810	**48.734**	**43.00**

This higher PSNR value generally indicates that the reconstruction is of higher quality.

Histogram for frame

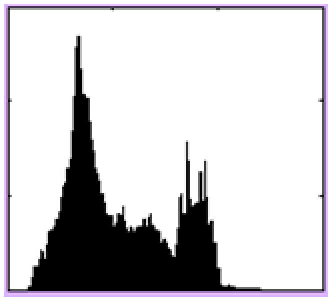

Fig 3: Histogram before data hiding

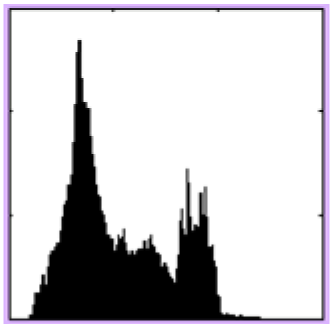

Fig 3: Histogram after data hiding

There are some differences between the above two histograms so it indicates the presence of some content inside the video

Fig 4:Before hiding

Fig 4:After hiding

There is no difference between the above two figures.So the security of the system is very high.So one of the major advantage of this sytem is doubling of security.Here attackers can't easily tamper the data inside the video..By using this video steganography we can increase the security of adaptive region incrementing visual cryptography

CONCLUSION

Steganography is the procedure of hiding information in digital media in order to hide the presence 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] J. Kodovsky, J. Fridrich, and V. Holub, \Ensemble classi_ers for steganalysis of digital media," Information Forensics and Security, IEEE Transactions on, vol. 7, no. 2, pp. 432{444, 2012.

[2] R.-Z. Wang, \Region incrementing visual cryptography," Signal Processing Letters, IEEE, vol. 16, no. 8, pp. 659{662, 2009.

[3] M. Naor and A. Shamir, \Visual cryptography," in Advances in Cryptology|EUROCRYPT'94, pp. 1{12, Springer, 1995.

[4] K.-H. Lee and P.-L. Chiu, \An extended visual cryptography Algorithm for general access structures,"InformationForensics and Security, IEEETransactions on, vol. 7, no. 1, pp. 219{229, 2012.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R.Stinson,\Visual cryptography for general access structures," Information and Computation, vol. 129,no. 2, pp. 86{106, 1996.

[6] S. J. Shyu and H.-W. Jiang, \E_cient construction for region Incrementing visual cryptography," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 22, no. 5, pp. 769{777, 2012.

[7] C.-N. Yang, H.-W. Shih, C.-C. Wu, and L. Harn, \Out of region incrementing scheme in visual cryptography," Circuits and Systems for VideoTechnology, IEEE Transactions on, vol. 22, no. 5, pp. 799{810, 2012.

[8] T. Anila and M. Wilscy, \An extended region incrementing visual cryptography scheme using unexpanded meaningful shares," in Mining Intelligence and Knowledge Exploration, pp. 340{349, Springer, 2013.

[9] R. Doshi, P. Jain, and L. Gupta, \Steganography and its applications in security," International Journal of Modern Engineering Research (IJMER),vol. 2, no. 6, pp. 4634{4638, 2012.

[10] K. S. Jenifer, G. Yogaraj, and K. Rajalakshmi, \Lsb approach for video steganography to embed images," International Journal of Computer Science and Information Technologies, 2014.

[11] X. Wu and W. Sun, \Extended capabilities for xor-based visual cryptography," Information Forensics and Security, IEEE Transactions on, vol. 9, no. 10, pp. 1592{1605, 2014.