International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 6, June 2016

Wavelet: In Progressive Visual Cryptography with Water Marking For Efficient Transmission

[1] Najmi.A, [2] Devi V R

[1] Student- M.tech, Microwave & TV Engineering, Department of ECE, Kerala University, Thiruvananthapuram, India.

[2] Assistant Professor – Muslim Association College of Engineering, Department of ECE, Kerala University, Thiruvananthapuram, India.

***Abstract*— The storage and Security of data's now become a major thread in this Digital world. The security and storage of the data can be made by collectively dividing the data into encrypted modules and save it in multiple users and the combination of these modules only can produce it back. Progressive Visual Cryptography (PVC) is a special encryption technique deals with security of data as images which can be utilized to recover the secret image gradually by superimposing more and more shares. If we only have a few pieces of shares, we could get an outline of the secret image; by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively. PVC using unexpanded shares regenerates images of high quality. The security of this system can be even multiplied if the random looking shares are enveloped into some meaningful images and thus avoiding the hackers attention. In the proposed method, a digital watermarking technique is used to generate meaningful images and Discrete Wavelet Transform for efficient encoding. The secret image shares are embedded on wavelet coefficients of the different cover images. At the de-embedding side the shares are extracted from the cover images and stacked one by one which reveals the secret image progressively. This scheme provides a more efficient way to hide images in different meaningful shares providing high security and recovered image with high contrast.**

***Keywords*—Visual Cryptography, Water marking, Data hiding, Cryptography**

I. INTRODUCTION

Embedding a secret image is an efficient and robust manner has a high priority in various fields. Here with the help of visual cryptography, watermarking and by wavelet decomposition one can achieve loss less and efficient way of communication. Visual Cryptography is an encryption technique to hide secrets in images in such a way that it can only be decrypted if and only if the correct key image is used. Here the secret data is divided into several shares and transmitted. Shares are stacked together to recover the original image data. Visual cryptography helps to recover a secret image by stacking two or more transparencies. In VC approach, the secret was divided into n shares, and each time one would receive only one share. Only when k or more shares of a secret are stacked together, the secret image can be retrieved correctly. One cannot retrieve the secret image if the number of stacked shares is less than k. This is known as (k, n) threshold mechanism.

In progressive visual cryptography (PVC) one can recover the secret image gradually by superimposing more and more shares. If one have only a few pieces of shares, then he could only get an outline of the secret image. By stacking more and more shares, the details of the hidden data can be retrieved progressively. Even though no one can decode hidden information from a single share or shares less than k, this technique is not that secure as the shares generated are noisy (random looking) images and have more interest of hackers as they can understand it as critical information in the transmission. If the noisy shares are enveloped into some meaningful pictures the interest of hackers can be reduced. Watermarking is a nice technique to hide these shares into meaningful pictures with the help of cover images. If the shares are embedded into the wavelet coefficient of cover image then the interest of hacker can be reduced as they can hardly have any clue of a hidden secret present in the cover image. Usage of wavelet can reduce losses and can cause lossless and efficient transmission.

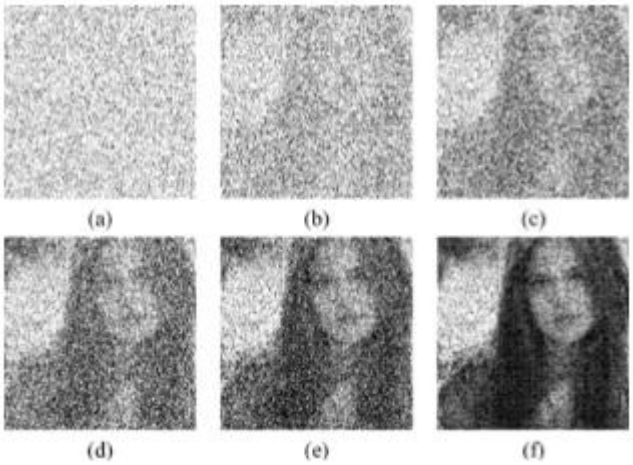

Fig 1.1 pvc with unexpanded share (Mena is reconstructed by stacking different numbers of shadow images. (a)–(f) Any 1–6 shadow images stacked.)

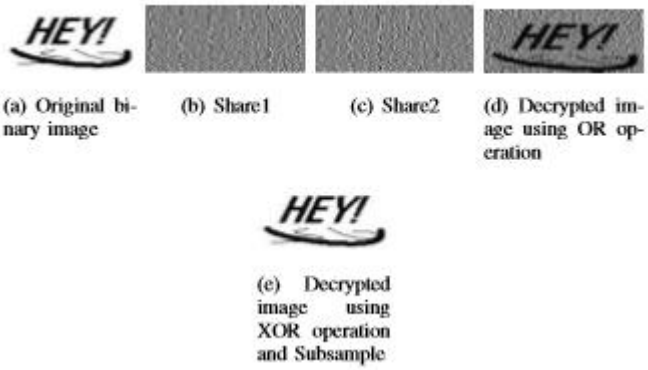

Fig 1.2 Example of (2,2) VCS scheme for binary image

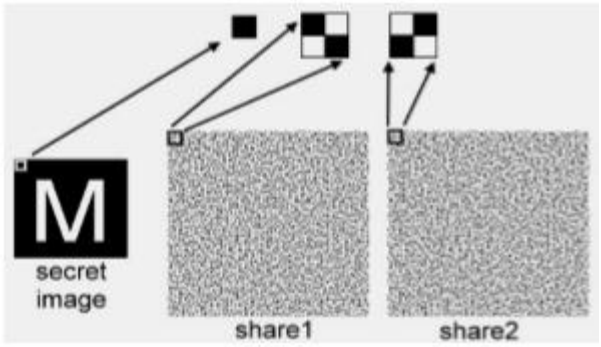

Fig 1.3 (2,2) Visual cryptographic scheme

Jithi P V and Anitha T Nair discussed a way to hide images in different meaningful shares so that high securely and a clear recovered image with high contrast can be assured. But PVC using unexpanded shares increases bandwidth and also transmission losses are there. Naor and Shamir proposed a new cryptography, called visual cryptography (VC) which attempts to recover secret image via the human visual system by stacking two or more transparencies. In their approach, the secret was partitioned into n shadow images (shares), and each participant would receive only one share. Once any k or more shares of a secret are stacked together, the secret image will be visually retrieved without the help of the computer. But this method uses pixel expansion to create shares, which would cause a problem of wasting the storage space.

Generally, a watermark embedded in the frequency domain is more robust than that in the spatial domain. The frequency domain transform techniques are more popular due to the natural framework for incorporating perceptual knowledge into the embedding algorithm which achieves better perceptual quality and robustness. Here we use a blind watermarking scheme that operates in the frequency domain. The watermark is masked according to the characteristics of the human visual system (HVS), taking into account the texture and the luminance content of the image subbands. We apply wavelet transformation on Luminance channel of color image and get the first level decomposition. From this a subband having high texture energy is selected. On this subband, apply DWT to obtain second level decomposition. From this, again select a subband having high texture energy and then embedd the watermark.

After embedding the watermark the texture properties of modified subband coefficients are recalculated to decide the noticeable distortions of image. If the change in texture property is high, then the embedding scaling factor is adjusted until the texture distortion is negligible. Thus, to maintain the perceptual similarity between the original color image and watermarked color image the embedding scaling factor is adjusted dynamically. In this scheme, we use VCS- (2,2) with Adaptive Order Dither Technique. Note that in our scheme, one of the share is directly embedded into cover image unlike in other schemes where the share image is preprocessed using a transform before embedding. The main feature of our scheme compared to other schemes is that the watermark is not expanded by factor of 2. Further, the proposed scheme resists different types of attacks.

In the proposed method we combine PVC with wavelet transforms for high security and lossless transmission.

II. RELATEDWORK

The conventional VC [1] applied the method of pixel expansion to create shares, which would cause a problem of wasting the storage space. Ito et al [3] combined the concept of probability with the conventional VC [15-16] to generate a share of invariant size. They introduced a method suitable for binary images. They used a scheme to encode black and white images into same sized shares as secret image.

Hou et al [9] used the method of reducing the contrast of gray-level images and the halftone technique to create pixel unexpanded shares. Shyu et al [4] used random grid and halftone technique to produce shares. In paper by Yi-Chang, Li, Yi- Chunand Juan [12], two Secret images are encrypted at the same time. This scheme turns two secret images into two meaningless shares without any pixel expansion and codebook. To restore the two secret images, users can directly superimpose these two shares to disclose the first image. To restore second share, superimpose the same two shares in a way moving horizontally one share. This reduces cost of transmission bandwidth and storage.

Tu and Hou[10] proposed a multipixel encoding method which could recover the gray-level or colored images with better visual quality. Hou used halftone technique and color composition/decomposition to simulate the gray scale of an image, thus solved the problem of Naor and Shamir's method which could only be applied to black and white images.

Thien and Lin [8] improved Shamir's theorem by using r pixels of a secret image as the coefficients of a r-1 degree polynomial, and, consequently, reduced the share size to 1/r. Based on the conceptions of [8], Chen and Lin [13] and Fang [14] each proposed a different progressive secret sharing scheme, using the techniques of reordering the bit-planes and discrete cosine transformation of an image, respectively. References [18], [8],[13-14] provided perfect ways to share information and [13] and [14] could even obtain the objective of displaying the secret image progressively. Nevertheless, all these schemes needed computer to solve those complicated math in order to decrypt the secret image other than simply using the human eyes.

III. METHODOLOGY

Here a secret image is divided into shares. The secret image shares are embedded on wavelet coefficients of the different cover images. The image is transformed into the frequency domain using the Haar wavelet transform, then the image sub-bands are encrypted in a such way that guarantees a secure, reliable, and an unbreakable form. The encryption involves scattering the distinguishable frequency data in the image using a reversible weighting factor amongst the rest of the frequencies. It shuffles and reverse the sign of each frequency in the transformed image before the image frequencies are transformed back to the pixel domain. . The decryption algorithm reverses the encryption process and restores the image to its original form. At the receiver side the shares are extracted from watermarked image and stacked one by one to get the secret share.

IV. PROPOSED HIDING ALGORITHM

A. Input secret message and cover signal

The secret message can be any text file or image and then inputting the cover signal in which data is to be embedded. This cover signal must be sufficient large to cover the message. After selection of input secret message and cover signal next, we find out the length of the image file as well as length of the text file.

B. Encryption

Before hiding the secret message into cover signal it must be converted into the other form so that it can't be interpretable by intruder. To do so first, we convert the secret data or message into multiple pieces called shares by using the method of progressive visual cryptography.

Algorithm

Input: A W × H halftone secret image P where p (i, j) P

Output: n shares Sm, m=1, 2, …. ,and n

Process:

1). Generate sharing matrices C0 and C1

2). For each pixel p (i, j), 1<=i<=W, 1<=j<=H

2.1). Randomly choose a value l, range from 1 to n

2.2). For m=1, 2,….,and n

2.2.1) If the pixel p (i, j) = 0 (white), the pixel value Sm(i,j) = C0(l,m)

2.2.2) If the pixel p (i, j) = 1 (black), the pixel value Sm(i,j) = C1(l,m)

Algorithm for watermarking

Input: Message

Output: Watermarked image

Process:

1. a. Read respective cover image

b. Do for each pixel

i. If share pixel is black

i.a. Set LSB of cover image pixel to 1

ii. If share pixel is white

ii.a. Set LSB of cover image pixel to 0

C. Cover Signal Segmentation

Let the input cover signal consist of R samples, this signal is segmented into two catagories: Processed samples and Unprocessed samples. The size of processed samples is depending on the size of the secret message. If the size of message is N then The Processed samples consist of N*2^L samples. Where L is decomposition level. the rest samples is called unprocessed samples, Next the processed part is partitioned into segments of size same as size of message that is N segments; each segment has length of Z samples

D. Segment Decomposition and Coefficient Selection

Each segment of the input image cover signal is decomposed using L level of Haar DWT transformation to obtain 2^L signals, each one of the produced signal has length of Z/2^L samples. One represents the Approximated signal and the others represent detailed signals. From the detailed signal we select one of the detail signals for embedding process. Length of approximated signal and detailed signal is Floor((n-1)/2) + N, where n is length of signal and N is related to no of filters.

E. Message Embedding Stage

The working for embedding the message is given below: If the secret message that is to be embedded is 0 then compare the selected coefficient with threshold value T and if coefficient is greater than T, then modify the value of coefficient so that it could become less then T. if it is not so then there is no need to change the value of coefficient. If the secret message that is to be embedded is 1 and if selected coefficient is less than threshold T, then modify the value of coefficient so that it could become greater than or equal to T otherwise there is no need to modify the coefficient. if S(i)==1

cd(4) = (cd(4))+.01; end

F. Watermarked image Reconstruction Stage

In this stage all the modified segments, are converted back from frequency domain to time domain. The IDWT is used to reconstruct the segments of - signal based on modified detailed coefficient and unmodified approximate coefficient. The reconstructed segments will fed to segment collecting step to reconstruct the final algorithm output.

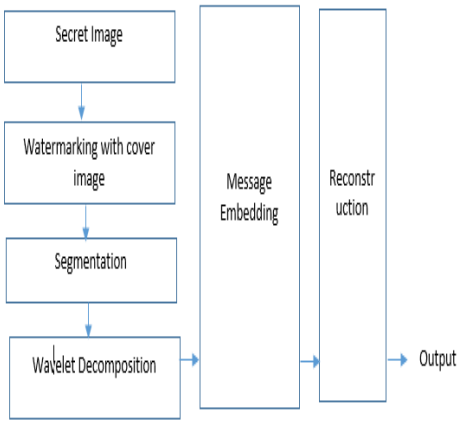

Fig. 3.1. Block diagram of the Message Hiding Algorithm.

V. MESSAGE RECOVERY ALGORITHM

The extraction process is divided into blocks : segmentation, decomposition, Coefficient selection, message extraction and reverse encryption.

A. Input Image signal

In the message recovery algorithm, first we select the Image signal from which data is to be extracted. This signal must be same as we have stored the signal in message hiding process.

B. Segmentation

Again, the signal is segmented into two categories: Processed samples and Unprocessed samples. The size of processed samples must be same as size of processed samples in hiding process. Size of processed samples is calculate by multiplying the size of message s with 2^L, where L is the wavelet decomposition level. Next the Processed part is segmented again into N segments; each segment has length of Z samples

C. Segment Decomposition and coefficient selection

Again, each segment of the image signal is decomposed using L level of Haar DWT to obtain 2^L signals, each one of the produced signal has length of Z/2^L samples. One represents the Approximated signal and the others represent detailed signals. From the detailed signal we select same detail signal that was selected on the time of hiding stage for embedding process

D. Secret Message Recovery Stage

Secret message recovery stage is very simple and based on comparison of selected detailed coefficient with threshold value T .If the coefficient is greater than or equal to threshold T it means that LSB of cover image is 1 otherwise it is 0

if(Segment(i,p)>=T)
LSB of cover image(i)=1;
elseif(Segment(i,p)<T)
LSB of cover image(i)=0;
End

E. Reverse Encryption

Before delivery of the secret message to receiver , it must be converted back to it's original form . Here the shares extracted from cover image is stacked one by one to generate secret image of high quality.

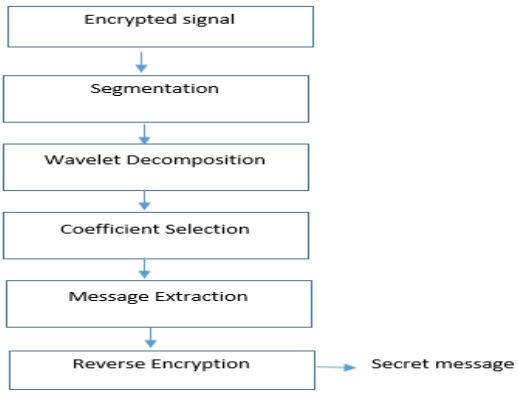

Fig. 3.2. Block diagram of the Message Recovery Algorithm.

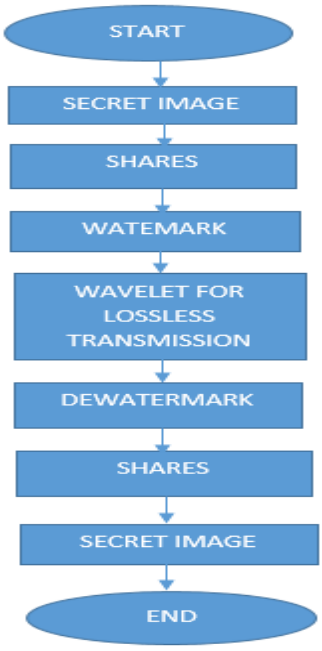

Fig 3.3: Flow Chart

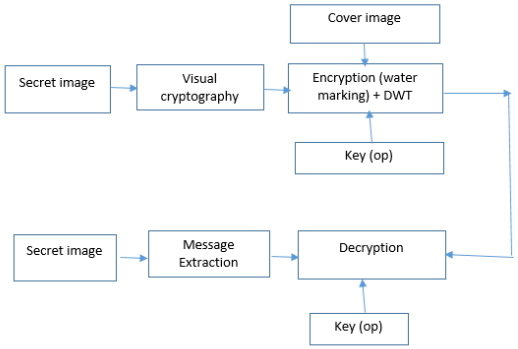

Fig 3.4: Block Diagram

VI. *RESULTS AND DISCUSSIONS*

Here a visual cryptography and digital watermarking technique is used to generate meaningful shares. Here a secret image is divided into shares. The secret image shares are embedded on wavelet coefficients of the different cover images. At the de-embedding side the shares are extracted from the cover images and stacked one by one which reveals the secret image progressively. This scheme provides a more efficient way to hide images in different meaningful shares providing high security and recovered image with high contrast.

Transmitter

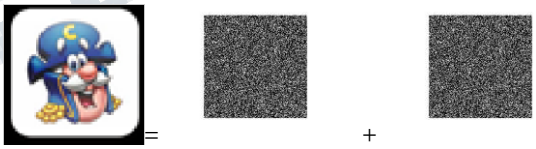

Fig 4.1 Visual Cryptography

Fig 4.2 : Watermarking

Receiver

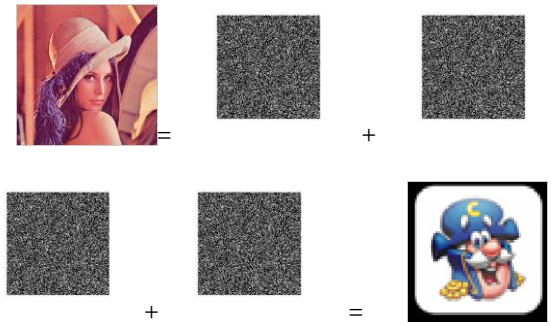

Fig 4.3: Decryptography

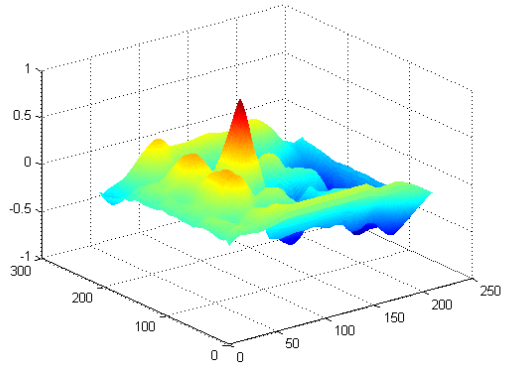

Fig 4.4: Graph showing variance

Here the graph shows variance almost zero, i.e if the variance is zero then that means correlation is high, That means lossless transmission has taken place.

VII. CONCLUSION

In this way, we have presented a new method by using the combination of visual cryptography, watermarking and wavelt decomposition. Here watermarking and progressive visual cryptography has been used for security and haar wavelet is used for lossless transmission and bandwidth efficiency. Thus it provides robust and secure way of communication with lossless transformation. Transmission of images with larger size with high resolution and less noise is the subject of future work.

Acknowledgment

I would like to express my sincere gratitude and heartfelt indebtedness to my guide for his valuable guidance and encouragement in pursuing thesis.

I am thankful to Head of the Department, Department of Electronics and Communication Engineering, Muslim Association College of Engineering for his help and support.

I also acknowledge my gratitude to other members of faculty in the Department of Electronics and Communication Engineering and all my friends for their whole hearted cooperation and encouragement.

Above all I am thankful to the God Almighty.

REFERENCES

1. M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptol: EUROCRYPT, vol. 950. 1995, pp. 1–12.
2. Shang-Lin Hsieh, I-Ju Tsai, Bin-Yuan Huang, and Jh-Jie Jian, Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform, Journal of Multimedia, vol. 3, No. 4, 2008, pp. 42-49.
3. R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography,"IEICE Trans. Fundamentals Electron., Commun. Comput.Sci., vol. E82-A, no. 10, pp. 2172–2177, 1999.
4. S. J. Shyu, "Image encryption by random grids," Patt. Recog., vol. 40,no. 3, pp. 1014–1031, 2007.
5. "Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based (k,n)-VCS" by Arti , Harsh K Verma ,International Journal of Computer Applications (0975 – 8887) Volume 46– No.9, May 2012
6. D. Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, pp. 1–13, 2005.
7. "Multi-pixel Visual Cryptography for color images with Meaningful Shares" by Ms. Kiran Kumari et. al. / International Journal of Engineering Science and Technology Vol. 2(6), 2010, 2398-2407
8. C. C. Thien and J. C. Lin, "Secret image sharing," Comput. Graphics,vol. 26, no. 5, pp. 65–770, 2002.
9. Y. C. Hou, C. Y. Chang, and C. S. Hsu, "Visual cryptography for color images without pixel

expansion," in Proc. CISST, vol. I. 2001, pp. 239–245.

10. S. F. Tu and Y. C. Hou, "Design of visual cryptographic methods withsmooth-looking decoded images of invariant size for gray level images,"Imag. Sci. J., vol. 55, no. 2, pp. 90–101, 2007.

11. W. P. Fang and J. C. Lin, "Progressive viewing and sharing of sensitiveimages," Patt. Recog. Image Anal., vol. 16, no. 4, pp. 638–642, 2006.

12. "Two image random encryption "by Yi-Chang,Li,Yi- Chunand Juan IEEE Transactions

13. 13. S. K. Chen and J. C. Lin, "Fault-tolerant and progressive transmission of images," Patt. Recog., vol. 38, no. 12, pp. 2466– 2471, 2005

14. 14. W. P. Fang, "Multilayer progressive secret image sharing," in Proc. 7thWSEAS, 2007, pp. 112–116.