Visual cryptography for gray scale images with enhanced security mechanisms

V. Lakshman Narayana[1,*], A. Peda Gopi[2]

Department of CSE, Vignan's Nirula Institute of Technology and
Science For Women, Guntur, Andhra Pradesh, India

lakshmanv58@gmail.com

ABSTRACT. *Security has gained a lot of importance with the rapid de velopment of communication/storage technology. Protecting the data has become an important issue. To provide more security to the image information, in this paper an enhanced security system has been proposed. Here the secret image is encrypted and transmitted by using a combined technique that make use of Discrete Wavelet Transform (DWT), Visual Cryptography (VC) and Water marking. DWT is first used for the compression of the secret image. The compressed image is used for further visual cryptographic process. VC encodes visual information into noise like shadow images called shares. By stacking the shares together the secret image can be visually decoded. Digital watermarking is used to provide additional security for the secret image. The generated shares are made invisible by using watermarking which also provides authentication for the shares. Different image types are used to evaluate the performance of the proposed scheme. Comparison with different values of scaling parameter M which is used to decrease the size of image in the VC is also done. The results clearly indicate that the proposed scheme can send more data with less bandwidth more secretly.*

RÉSUMÉ. *La sécurité a pris beaucoup d'importance avec le développement rapide de la technologie de communication / stockage. La protection des données est devenue un enjeu important. Pour renforcer la sécurité des informations sur les images, un système de sécurité amélioré a été proposé dans cet article. Ici, l'image secrète est cryptée et transmise à l'aide d'une technique combinée utilisant la transformation en ondelettes discrète (DWT), la cryptographie visuelle (VC) et le filigrane. DWT est d'abord utilisé pour la compression de l'image secrète. L'image compressée est utilisée pour un processus cryptographique visuel ultérieur. VC code des informations visuelles en bruit, telles que des images d'ombre appelées des partages. En empilant les partages ensemble, l'image secrète peut être décodée visuellement. Le filigrane numérique est utilisé pour renforcer la sécurité de l'image secrète. Les partages générés sont rendus invisibles à l'aide d'un filigrane qui fournit également une authentification pour les partages. Différents types d'images sont utilisés pour évaluer les performances du schéma proposé. Une comparaison avec différentes valeurs du paramètre de mise à l'échelle M utilisé pour réduire la taille de l'image dans le VC est également effectuée. Les résultats indiquent clairement que le schéma proposé peut envoyer plus de données avec moins de bande passante de manière plus secrète.*

KEYWORDS: *visual cryptography, DWT, digital watermarking.*

MOTS-CLÉS: *cryptographie visuelle, DWT, filigrane numérique.*

DOI:10.3166/TS.34.197-208 © 2017 Lavoisier

1. Introduction

The privacy of information to be transmitted is becoming more and more important, because of the rapid progress in data exchange through public domain. For the privacy of data, Visual Cryptography (VC) is a good choice. The idea behind visual cryptography is to divide an image into random shares. Individually these shares will not reveal any information about the original image (Naor and Shamir, 1995). These shares are composed of black and white pixels and by superimposing these shares together the original image can be recovered. This work is motivated by the earlier works available in literature. Considerable amount of work is done in this area and some methods have been developed. As a new secret sharing technique, Visual Cryptography Scheme (VCS) was first introduced by Naor and Shamir in Euro-Crypt conference in 1994 (Naor and Shamir, 1995). Here n-shares are generated from a binary secret image in the encoding section. In the decoding section to reveal the binary secret image k or more than k shares are stacked together. (Verma and Dr, 2012), (Ranjan-Kumar *et al*., 2013; Wang *et al*., 2014) proposed different VC techniques such as two share creation , residual number system based on Chinese Remainder Theorem and Tagged VC for hiding tag images respectively. Digital watermarking is an effective method used to determine the ownership of the image by taking the raw image data and embedding some private information into it. Invisibility and stability are two significant features of digital watermarking. (Madhusudhana and Sapna, 2015) proposed a four share creation VC using augmentation method and Singular Value Decomposition (SVD) and frequency domain watermarking technique. Ayan Banerjee et al (Ayan and Sreya, 2012) proposed a technique of combining the block optimization VC and blind invisible watermarking technique.

Huge volume of data has to be stored and transferred, with the increasing use of digital images. The transmission bandwidth and storage capacity required by the uncompressed image is considerable. By compression techniques the redundant information present in the images is removed with less degradation in the quality of the image. Wavelets are used for encoding information Wavelets are also used as mathematical tool for hierarchically decomposing functions. Here 2D-Haar Discrete Wavelet Transform (DWT) which is a low complex 2D compression method using wavelets is used. Kamrul Hasan *et al.*, K.L. Sudha *et al.* proposed Haar compression and steganography using chaos techniques in (Talukder and Harada, 2007; Sudha and Bhavana, 2012; Sudha and Bhavana, 2012) respectively.

The scheme proposed combines the qualities of compression, VC and watermarking. The main aim of this scheme is to reduce the bandwidth required for transmission this is achieved by compression using DWT .The secret shares generated by using VC further reduces the size of the shares when compared to other techniques. These shares are subjected to invisible watermarking which protects the secret shares.

During decryption the shares are extracted and are stacked together to get back the compressed image. The original secret image is obtained by Inverse DWTSection II deals with the proposed method, Section III shows the results and discussions.

2. Literature work

Barely any asks about have inspected the VC for grayscale and shading pictures. Naor and Shamir made reference to the augmentation of their arrangement to grayscale images. That is, to speak to the dim dimensions of the covered picture by controlling the way how the dim subpixels of the sheets are stacked together. The grayscale form of the VC is in a general sense proposed in the paper. There are a couple of request about that deal with shading images. Naoret.alanalyzed the VC conspire which changes a message with two tones, by engineering the toned or straightforward subpixels. Koga *et al.* formulated cross area based (k, n) scheme. The methodology by Verheul et.alis basically like Koga's. The two methodologies allocate A shading to a subpixel at a specific position, which implies that showing m hues utilizes $m-1$subpixels.

The subsequent pixels contain one hued subpixel and whatever remains of the subpixels are dark. Hence the more hues are utilized, theworse the differentiation of the pictures moves toward becoming significantly. Their approaches can't be connected tothe expanded VC, either. Rijmenet.al discussed empowering multicolours with moderately less subpixels. Anyway every sheet must containcolor arbitrary pictures, which implies applying this way to deal with the all-inclusive proposed around the (3, 3) conspire and discusses the technique to manage the common pictures with middle of the road graylevels. It likewise demonstrates howto upgrade the difference. In Hou proposes a VC (Ranjan-Kumar *et al*., 2013) for shading pictures. There have been many distributed examinations of VC.

A large portion of them, in any case, have focused on talking about high contrast pictures, and only few of them have proposed strategies for handling dark dimension and shading pictures. Rijmen et.al have proposed a VC approach for shading pictures. In their methodology, every pixel of the shading mystery picture is ventured into a 2×2 square to shape two sharing pictures. Each 2×2 square on the sharing picture is Elled with red, green, blue and white (straightforward), separately, and subsequently no sign about the mystery picture can be recognized from any of these two offers alone. Rijman and Preneel guaranteed that there would be 24 conceivable blends as indicated by the change of the fou2.3. Dim dimension VC.Since most printers need to change dim dimension pictures into halftone ones preceding printing, and the changed halftone pictures are high contrast just, such a picture arrange is exceptionally reasonable for the customary technique to create the offers of VC. So in this paper, utilize changed halftone pictures to create the VC for dim dimension pictures. The calculation is asfollows: 1.

Change the dim dimension picture into a dark and-white halftone picture. 2. For each dark or white pixel in the halftone picture, break down it into a 2×2 square of the two transparencies In the paper of Visual Secret Sharing Scheme utilizing Grayscale

Images By Sandeep Katta (Talukder and Harada, 2007) in proposes a probabilistic 2-out-of-3 visual mystery sharing plan for grayscale pictures and gives a superb pictures that of flawless quality to be remade. Here as of now examining to change the grayscale mystery sharing plan in to most effective way. In this plan the nature of the picture is kept up flawlessly with no loss of sweeping statement yet the span of the shadow is expanded radically, which speaks to the pixel extension issue.

Mystery sharing methods have a place with the bigger zone of data concealing that incorporates watermarking. In mystery sharing, irregular looking offers when united reproduce the mystery. In recursive mystery sharing, the offers themselves have segments characterized at a lower recursive dimension. The infusion of the arbitrary bits in the offers might be done advantageously utilizing d-successions or other irregular groupings. A grayscale picture is a picture in which the estimation of each single pixel is an example, that is, it conveys just force data. The darkest conceivable shade is dark, which is the aggregate nonappearance of transmitted or reflected light and the lightest conceivable shade is white. As indicated by their physical attributes, distinctive media utilize diverse approaches to speak to the shading dimension of pictures. The PC screen utilizes the electric flow to control gentility of the pixels. The decent variety of the gentility creates diverse shading levels. The general printer, for example, 2dot framework printers, laser printers, and stream printers can just control a solitary pixel to be printed or not to be printed, rather than showing the dim dimension. Accordingly, the best approach to speak to the dim dimension of pictures is to utilize the thickness of printed dabs. The strategy that utilizes the thickness of the net specks to reproduce the dark dimension is designated "halftone" and changes a picture with dim dimension into a twofold picture before preparing. Each pixel of the changed halftone picture has just two conceivable shading levels. Since human eyes can't distinguish excessively small printed dabs and, when seeing a dab, will in general cover its adjacent dabs, we can mimic diverse dark dimensions through the thickness of printed dabs, despite the fact that the changed picture really has just two hues – highly contrasting.

3. Proposed method

The proposed scheme is a hybrid algorithm which combines two different approaches DWT compression and VC together and which overcomes the limitation in the transmission bandwidth. The proposed algorithm as block diagram is shown in Figure 1.

First the secret image is compressed to half of its original size by using 2D-DWT compression technique. Then four shares are generated by using the VC model proposed. These shares can be generated by using different values of scaling parameter M. The shares are then embedded into four cover images to provide additional security to the secret image. The secret shares are extracted from the cover images during the decryption phase and inverse DWT is done to get back the original image.

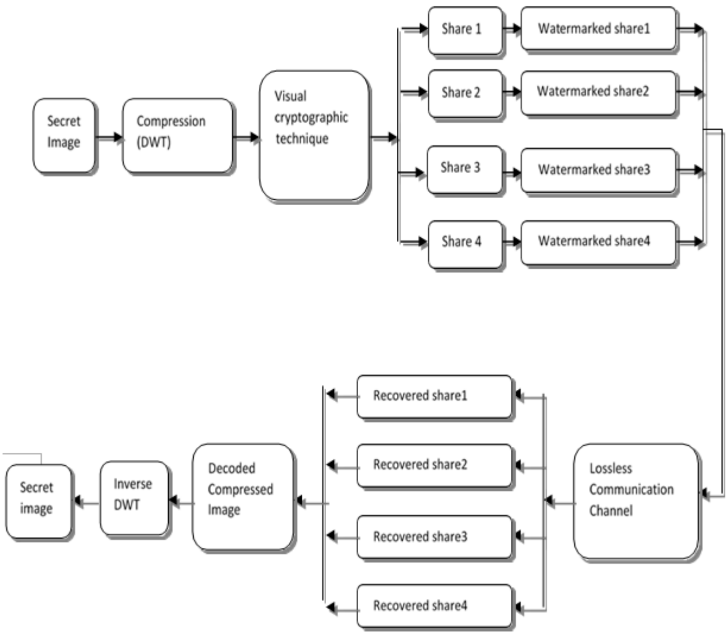


Figure 1. Architecture of proposed method

3.1. 2D-DWT

To view the spatial and frequency characteristics of multi resolution images a mathematical tool known as Discrete Wavelet Transform is used. The Discrete Wavelet Transform (DWT) used in this proposed scheme is Haar-DWT, the simplest DWT. Using Haar wavelet transform, an image II of size MM×NNp ixe ls is decomposed into four sub bands $LLLL$1, $LLHH$1,1 and $HHHH$1 having size X×Y. The low frequency component is the sub band $LLLL$1, which contains most of the energy of the image. The sub bands labeled$LLHH$1, HL1, and $HHHH$1 contain the higher frequency detail in formation (Kaur and Malotra, 2015; Ahmed *et al.*, 2016) The equations 1 to 4 represents the first four Haar sub

$$\mathrm{LL1(i,j)} = \frac{1}{4}\sum_{x=0}^{1}\sum_{y=0}^{1} I(2i+x, 2j+y) \qquad (1)$$

$$\mathrm{LH1(i,j)} = \frac{1}{4}\sum_{x=0}^{1} I(2i+x, 2j) - \frac{1}{4}\sum_{x=0}^{1} I(2i+x, 2j+1) \qquad (2)$$

$$\mathrm{HL1(i,j)} = \frac{1}{4}\sum_{y=0}^{1} I(2i, 2j+y) - \frac{1}{4}\sum_{y=0}^{1} I(2i+1, 2j+y) \qquad (3)$$

$$\mathrm{HH1(i,j)} = \frac{1}{4}\{I(2i, 2j) + I(2i+1, 2j+1) I(2i+1, 2j) - I(2i, 2j+1)\} \quad (4)$$

where(ii,jj) is the pixe l value at the coordinate $ii,jj$of II and $LLLL1(ii,jj)$, $LLHH1(ii,jj)$, $HHLL1$ (ii,jj) and $HHHH1(ii,jj)$ are the coefficients atthecoordinatesofthesubbands$LLLL1$,$LLHH1$,$HHLL1$and$HHHH1$ respectively. The two levels of compression that can be done using DWT is shown in Figure 2. In the proposedmethod one level of decomposition is considered, where the image size is reduced to half of its originalsize.

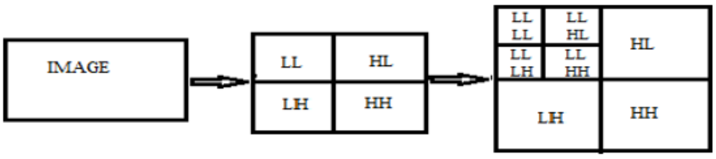


Figure 2. Two levels of compression using DWT

3.2. Visualcryptography

VCdecomposes the image into N number of shares and decryption is done by stacking these shares together (Babu *et al.*, 2013; Premkumar and Dinesh, 2012; Prashant *et al.*, 2014). In the proposed algorithm the input to the VCscheme is a compressed image C. The LL band of image C is considered as image C_1 , which is split into N shares in such a way that every pixel in $C_1$is represented by M number of bits in each of the N shares formed. This is done by dividing each pixel value of $C_1$by an integer so that new pixel values lie in the range 0 – 4M. Here M is used as a scaling factor which decides the BW of the transmitted pictures with shares. This new image is considered as C_2 .The pixel value x (i, j) in $C_2$is represented by N random numbers r(1),r(2),r(3) … r(N) in the range 1-M such that the sum of these random numbers gives that pixelvalue.

i.e. $\sum_{k=1}^{4} r(k) = x(i,j)$.Each random number isthen represented by M binary digits such that the number of 0's in these M binary digits is equal to the random number. These random numbers form the matrices$S_N$containing binary digits and are known as shares. The first random number of all the pixel values form the first share $S_1$and the second random number of all the pixel values form the second share $S_2$and so on .,In this way N random numbers generated will be used to formNsharesS_1,S_2….S_N.

3.3. Watermarking

Watermarking can be achieved in spatial domain or in frequency domain. In spatial domain embedding technique pixels of the image is modified directly (Datta *et al.*, 2013). In the proposed scheme LSB watermarking technique is used. Each share is watermarked on to different cover images whose size must be same or bigger than the size of the shares. The watermarking method replaces the LSB of every pixel of the grayscale cover images by the individual binary digits of the shares at the same position. For example if 200 is the pixel value of the cover image i.e11001000 and the individual binary value of the share is 1, then the LSB of the cover image pixel is replaced by 1 so that the first pixel of the watermarked image will become 11001001 i.e201 which will not affectthe quality of the cover image. Then approximately to hide the shares only half of the bits in a cover image will need to be modified. Thus 4 watermarked shares areformed.

3.4. Decryption

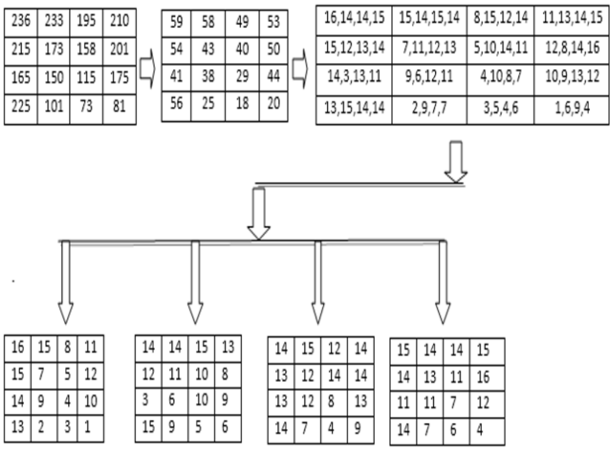
The watermark extraction principle is simple. The LSB bit of all the pixels from the watermarked image is extracted to get back the binary shares. In all the shares the blocks of M bits are collected and the number of 0's is counted to get back the grayscale shares. For M=16 the block of M bits say c = 1100010100011100 is considered, thenc' = NOT(c) and $\sum_{k=1}^{4} c'_k$ will give the pixel value i.e 9.The first pixel of each of the shares are added and multiplied by four to get backthefirst pixe l of the reconstructed compressed image. i.e

$4[\sum_{k=1}^{4} share\ k(i,j) = share\ K(i,j))]$For e xample, if the first pixel values of individual shares are 9,16,11,13 then reconstructed pixel value is 4*(9+16+11+13) = 196. This process is repeated for all the pixels of the shares to recover the whole image. Inverse DWT is then applied to obtain the reconstructed secretimage.

The encryption process for M=16 is e xplainedin detail by taking a part of the compressed image (4X4) given in table TableI. Each pixel value of the image is divided by an integer 4 so that new pixel value in the range 0 – 64 isgenerated

Then for each pixel value x (i, j), 4 random numbers r(1), r(2), r(3) and r(4) in the range 1-16 is generated. 4 Shares are generated by collecting first, second, third and fourth random numbersofeachpixelvaluesasgiveninTable 1.

Table 1. Share generation



236	233	195	210
215	173	158	201
165	150	115	175
225	101	73	81

59	58	49	53
54	43	40	50
41	38	29	44
56	25	18	20

16,14,14,15	15,14,15,14	8,15,12,14	11,13,14,15
15,12,13,14	7,11,12,13	5,10,14,11	12,8,14,16
14,3,13,11	9,6,12,11	4,10,8,7	10,9,13,12
13,15,14,14	2,9,7,7	3,5,4,6	1,6,9,4

16	15	8	11
15	7	5	12
14	9	4	10
13	2	3	1

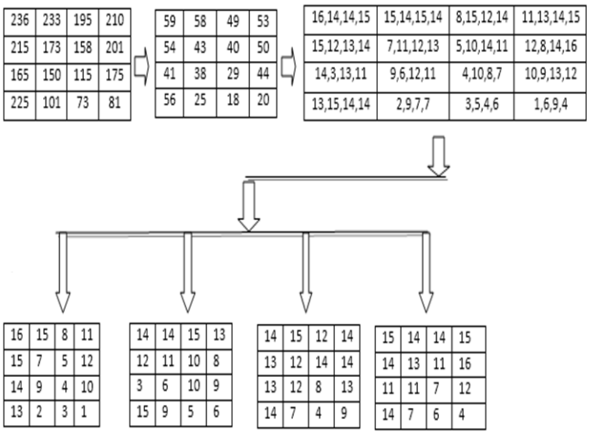
14	14	15	13
12	11	10	8
3	6	10	9
15	9	5	6

14	15	12	14
13	12	14	14
13	12	8	13
14	7	4	9

15	14	14	15
14	13	11	16
11	11	7	12
14	7	6	4

For each random number, 16 binary digits are generated. Such that the random number is equal to the number of 0’s. In this way 4 random numbers generated for every x (i,j) will be used to form 4 shares. Example of 2 shares are shown in Table 2.

Table 2. Example of two shares generated



236	233	195	210
215	173	158	201
165	150	115	175
225	101	73	81

59	58	49	53
54	43	40	50
41	38	29	44
56	25	18	20

16,14,14,15	15,14,15,14	8,15,12,14	11,13,14,15
15,12,13,14	7,11,12,13	5,10,14,11	12,8,14,16
14,3,13,11	9,6,12,11	4,10,8,7	10,9,13,12
13,15,14,14	2,9,7,7	3,5,4,6	1,6,9,4

16	15	8	11
15	7	5	12
14	9	4	10
13	2	3	1

14	14	15	13
12	11	10	8
3	6	10	9
15	9	5	6

14	15	12	14
13	12	14	14
13	12	8	13
14	7	4	9

15	14	14	15
14	13	11	16
11	11	7	12
14	7	6	4

4. Results and discussion

Matlab 10.0 tool is used to simulate the proposed algorithm for the transmission of secret image with VC combined with watermarking and DWT. Figure 3 depicts the input secret image of dimensions 256 X 256. This image is then compressed to the size 128 X 128 by using Haar technique as in Figure 4. Figure 5 and Figure 6 depicts the recovered compressed and original image respectively.

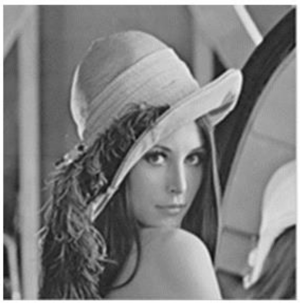


Figure 3. Inputsecretimage

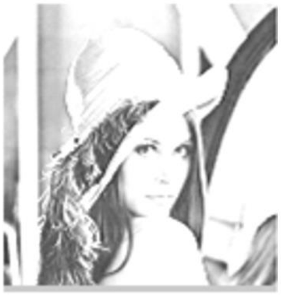


Figure 4. Compressedimage

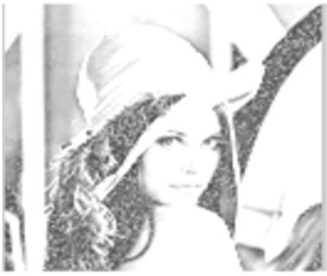


Figure 5. Reconstructed

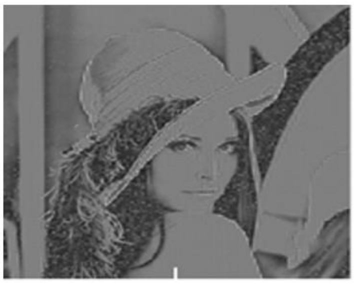


Figure 6. Reconstructed secretimage

Table 3. Bandwidth utilization for different values of M

Secret grayscale image size	M	Cover image size	PSNR
256 X256	16	512 X 512	24.3
	8	512 X 256	24
	4	256 X 256	23.5

Table 4. Comparison of total pixel value for different techniques

Methods	Type of image	Compression technique	Size ofthe singleshare		Total Pixel value
Basic VC	Binary	Not used	256 X 256X4		2,62,144
	grayscale	Not used	256 X 256 X 4 X 8		20,97,152
Proposed	grayscale	DWT	M =16	512 X 512	2,62,144
			M = 8	512 X 256	1,31,072
			M = 4	256 X 256	65,536

The same process explained in the proposed method can be donefor different values of M. In this work, three values of M are considered. The comparison Table III is shown to indicate the bandwidth utilizat ion for these values of M. The bandwidth required to transmit these visual cryptographic images can be reduced by using lower values of M, because the size of the cover images can be reduced according to the value of M. As the size of the cover image reduces, the bandwidth required to transmit these images is also reduced but variation in PSNR is negligible is shown in Table 3.

Comparison of bandwidth utilization of previous methods with the proposed method is shown in Table 4.

The bar graph for PSNR of different image types with different values of M is shown in Figure 7.

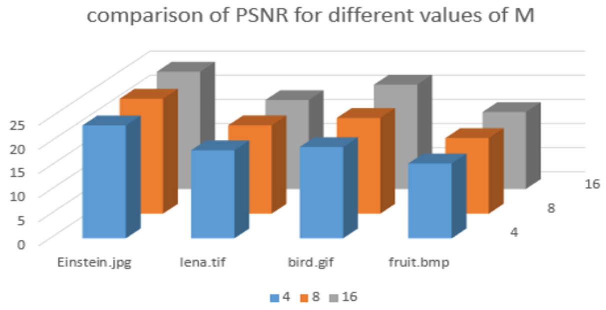


Figure 7. Bar graph of different image types

The main observation we can make from the above results is that the requisition of bandwidth reduces with negligible variation in the quality of the image. It can also be perceived that with only DWT and with DWT and VC the PSNR change is minimum. In the compression stage the size of the image is reduced to one half of its original size and further reduction is done by using M=4, which shows lesser bandwidth utilizat ion for transmission when compared to other VC methods. Another important observation is that decryption is a simple process which does not require complex computations. This reduces the complexity of the receiver section

From the above results it is also observed that the proposed method increases security due to 1) the generation of four shares 2) The visual cryptographic method which the hacker will not be knowing. 3) The conversion of the grayscale shares to binary shares is also unpredictable 4) the binary stuffing of the shares on to cover images does not reveal how the secret image is being transmitted.

5. Conclusion

The proposed scheme introduces a combined secret sharing system which uses compression, VC and watermarking techniques. While the cover image is holding the data, the secrecy of the data and the bandwidth required to transmit these images is a major concern. Thus in the proposed scheme transmission bandwidth is reduced by first applying compression technique and then using visual technique to the secret image before embedding it in the cover image. Performance parameters considered are the quantity of data which refers to maximum amount of data the can be sent and simplicity of the technique used. The proposed scheme is hybrid algorithm which combines two different approaches together that are DWT compression and VC which overcomes the limitation in the transmission bandwidth and provides multiple levels of security.

As future scope color images can be considered. Different attacks can be considered to find out the level of degradation of the image and find solutions to improve that.

Reference

Ayan B., Sreya B. (2012). A robust visual cryptography technique for photographic grayscale images using block optimization and blind invisible watermarking. *International Journal of Computer Theory and Engineering,* Vol. 4, No. 2.

Babu C. R., Sridhar M., Babu B. R. (2013). Information hiding in gray scale images using pseudo - randomized visual cryptography algorithm for visual information security. *2013 International Conference on Information Systems and Computer Networks*. https://doi.org/10.1109/ICISCON.2013.6524202

Kaur K., Malhotra S. (2015). Image compression using HAAR wavelet transform and discrete cosine transform. *International Journal of Computer Applications*, Vol. 125, No. 11, pp. 28-31. https://doi.org/10.5120/ijca2015906141

Madhusudhana B. S., Sapna P. J. (2015). Combined analysis of visual cryptography using SVD technique and frequency domain watermarking technique. *International Journal of Engineering Research & Technology*, Vol. 4, No. 5. https://doi.org/10.17577/IJERTV4IS050361

Naor M., Shamir A. (1995). Visual cryptography, advances in cryptology eurocrypt '94. *Lecture Notes in Computer Science,* No. 950, pp. 1-12. https://doi.org/10.1007/BFb0053419

Nashat A. A., Hassan N. M. H. (2016). Image Compression based upon wavelet transform and a statistical threshold. *International Conference on Optoelectronics and Image Processing*. https://doi.org/10.1109/OPTIP.2016.7528492

Premkumar S., Dinesh L. (2012). Efficient algorithm for steganography technique combined with image cryptography for secure application. *International Journal of Computer Applications*,Vol. 49, No. 13, pp. 45-48. https://doi.org/10.5120/7691-1011

Ranjan-Kumar H. S., Prasanna-Kumar H. R., Sudeepa K. B., Ganesh A. (2013). Enhanced security system using symmetric encryption and visual cryptography. *International Journal of Advances in Engineering &Technology*, Vol. 6, No. 3, pp. 1211-1219.

Sudha K. L., Bhavana S. (2012). Novel approach for Image steganography using Chaos published in Serials publicationsInternational. *Journal of Image Processing and Applications*.

Swadas P. B., Patel S., Darji D. (2014). A comparatively study on visual cryptography. *International Journal of Research in Engineering and Technology,* Vol, 3, No. 1.

Talukder K. H., Harada K. (2007). Haar wavelet based approach for image compression and quality assessment of compressed image. *IAENG International Journal of Applied Mathematics*, Vol. 36, No. 1.

Verma J., Vineeta K. (2012). A visual cryptographic technique to secure image shares. *International Journal of Engineering Research and Applications*, Vol. 2, No. 1, pp. 1121-1125.

Wang X., Pei Q. Q., Li H. (2014). A lossless tagged visual cryptography scheme. *IEEE Signal Processing Letters*, Vol. 21, No. 7. https://doi.org/10.1109/LSP.2014.2317706