Partial Image Secret Sharing Using Discrete Wavelet Transform

Abdelnaser Rashwan, Honggang Wang[*]

Electrical and Computer Engineering Department, University of Massachusetts Dartmouth, North Dartmouth, MA

Abstract   It is challenging to apply secret image sharing schemes for image transmission over wireless networks. Many of the existing secret images sharing schemes do not pay much attention to the relationship between the share size and share transmission. To reduce a share size and protect the image transmission, we propose a secret sharing scheme that uses a Discrete Wavelet transform (DWT) decomposing an image into low frequency and high frequency bands. Our proposed scheme can be applied in each frequency band individually to produce shares. Since the low frequency band has the significant coefficients of the image, in case of a share transmission over a lossy wireless channel, redundant shares are only taken from the low frequency bands to mitigate the loss in the reconstructed image. Since the I-frame in MPEG codec is the most significant frame and all other frames in the video sequence are referenced to it, we apply our secret scheme in this frame to secure video sequence. We use our simulation to prove the efficiency of the proposed schemes.

Keywords   Secret images sharing, Discrete Wavelet transforms

1. Introduction

With the fast development of various types of communication networks, there is an increasing demand to secure the data transmission. Users want to keep their data secure from unauthorized users. This always requires using some encryption techniques such as data hiding and steganography. However, many of these protection schemes are not designed for the image transmission over wireless networks. If an unauthorized user obtains the encryption key, then it will become easy for him/her to obtain an access to the whole data of interest. Moreover, saving sensitive information in just one storage node would not be efficient if that node is subject to physical damage.

Secret image sharing schemes have been implemented to protect secret images from being compromised. Secret sharing schemes have an advantage over the aforementioned schemes where in secret sharing schemes, even if the unauthorized user has access to some data, he/she will not be able to decrypt the whole data of interest.

Shamir [1] first hypothesized the secret sharing. The author named his new approach the (T, N) threshold scheme. The threshold scheme splits the secret data into small pieces called "shares". The secret data could be only reconstructed by using a number of shares no less than a defined threshold T. In [11] Brinkman et al. have suggested a secret sharing

scheme to look for the image contents in encrypted data. It is also shown how to securely retrieve the image at receiver using Shamir. Bai [2] also suggested a scheme by using matrix projection with Shamir's scheme. Lately, Wang et al. [3] proposed an incrementing visual cryptography by employing random grids. Chen and Tsao [4] designed a threshold RG-based on visual secret sharing scheme. To reduce the share size, Thein and Lin [3] suggested numerical processing procedures to share a secret image secretly where they initially permute an image into random image and then shares. Shares are generated using a secret sharing approach proposed by Shamir. They succeeded in reducing the share size to 1/T of the original image. In [15], Huffman code was used to reduce the share size. In addition, there are some research works using the secret sharing for secure data transmission. However, they did not pay attention to the secret sharing sensitivity to errors and how that packet loss could degrade the reconstructed image quality.

In terms of multimedia encryption, many encryptions schemes are proposed to protect the video [6] [17]. In [11], Qiao and Klara suggested splitting a group of I-frame packets into two parts and then both parts are XORed and saved in one part. The other part was encrypted with Data Encryption Standard (DES). In [10], Chen improved this scheme by changing the permutation range from a segment to a frame. Chen also proposed to divide each DCT macro-block into 64 groups according to their positions, and scrambled them within each group. In [16], the authors proposed to design secret sharing based on the DC coefficients and AC coefficients. However, it is very challenging to apply these schemes in real-time image

streaming application when the image or video size is large. There are many existing works for multimedia transmission over networks [18-23]. In these works, the transmission quality and network quality of service are major goals.

As we mentioned earlier that secret sharing schemes are sensitive to channel errors because losing one pixel in a share results in losing T pixels in the reconstructed image. To combat this quality degradation in the reconstructed image, redundancy will be needed and with rate higher than redundancy in traditional encryption schemes. It is clear that high redundancy is not efficient if these schemes are used in resource constraints systems. For this reason, we adopt a discrete wavelet transform (DWT) to reduce the redundancy size by shrinking the size of the shares where the secret image is transformed by DWT to pro-duce one low frequency band and three high frequency sub-bands. Then, Thein and Lin's scheme can be applied in each band separately to produce shares for each sub-band. The redundant shares would be only transmitted from the low sub-band because it has the most significant coefficients of the image. By this way, we ensure that the redundant shares size decreases and many resources (i.e., energy, bandwidth) can be reduced. Obviously, small share size also adds some flexibility to the framework in terms of transmission speed. Experimental results show that the proposed scheme successfully decreases the shares size while providing the same image quality at the same level as the Thein and Lin's scheme.

Decoding the Inter-frames (P-frames, B-frames) in the video sequence cannot be achieved without successful decoding of Intra-frame (I-frame). Therefore, we suggest securing the video sequence by applying secret image sharing only on the I-frame to produce the shares. The inter-dependency between the I-frame and inter-frame (P-frame, B-frame) is exploited to develop a video quality metric based on secret image sharing.

The remaining sections are organized as follows. A brief review of Thien and Lin's scheme is given in section 2. In Section 3, the proposed work will be described in details. We discuss the experimental results in Section 4. Finally, Section 5 concludes this paper.

2. Thien and Lin's Scheme

Thein and Lin scheme generated N shares by splitting the secret image (main image) into π non overlapping T blocks, each block is represented in the corresponding shares representation as shown below:

$$y_i(x) = (a_{i_0} + a_{i_1}x + a_{i_2}x^2 + ... + a_{i_{(T-1)}} x^{T-1}) \bmod 251 \quad (1)$$

Where $y_i(x)$ indicates the share pixel connected with i^{th} block in the share image, for $0 \le i \le \pi$ and $1 \le x \le N$. The value of $y_i(x)$ is obtained using the original pixel values that are contained in the ith block. Truncating the values of the share pixels by dividing every pixel by 251(251 is the largest prime number in the uint8 gray image). Because the degree of the polynomial is chosen to be T-1, the size of share is $1/T$ of the secret image. To reconstruct the secret image, The polynomial in Eq.(1) can be retrieved by Lagrange interpolation. Repeating these procedures for all shares pixels reconstruct the secret image.
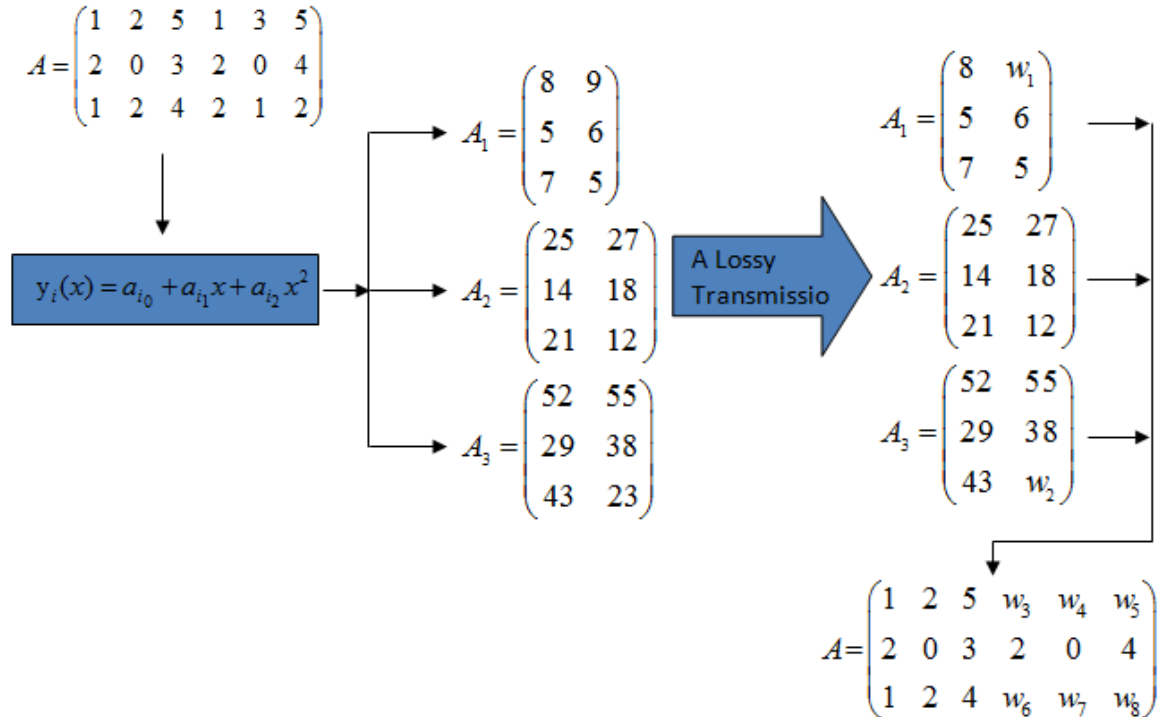

Figure 1. An example of distorted shares

3. Partial Image Secret Sharing

Most of the existing secret images sharing schemes did not pay attention to share transmissions over wireless networks. The question here is: if the shares are received with some distortion, can uses still be able to reconstruct the original image? A corrupted share means that there are some distorted pixels in the share. In Fig.1, a secret matrix A is divided into three shares by using a secret threshold (T=3, N=3). This threshold indicates that the polynomial will be with a degree of 2. Therefore, three points are needed to define this polynomial. When one of the three points is lost, it becomes impossible to derive the polynomial formula.

As it can be seen in Fig.1 that losing one element in a share A_1 results in losing three elements in the reconstructed matrix. Because losing one pixel in the share leads to losing T pixels in the reconstructed images, high redundancy becomes necessary to mitigate the loss in the reconstructed image. Transmitting redundant shares with a size equal to the Thein and Lin' share size (size of Thein and Li's share is (main image size/T)) can be exhaustive for resource constrained networks. For this reason, we suggest improving Thein and Lin's scheme by using DWT. DWT is a transform technique that divides the main image into one low frequency (green dotted box in Fig. 2) band and three high frequency bands (red dotted box as illustrated in Fig. 2). Thein and Lin's scheme is applied on each band individually to generate the shares. In the proposed scheme, redundant shares with a size of (main image size/4T) are only taken from low frequency band because it has the most significant coefficients.
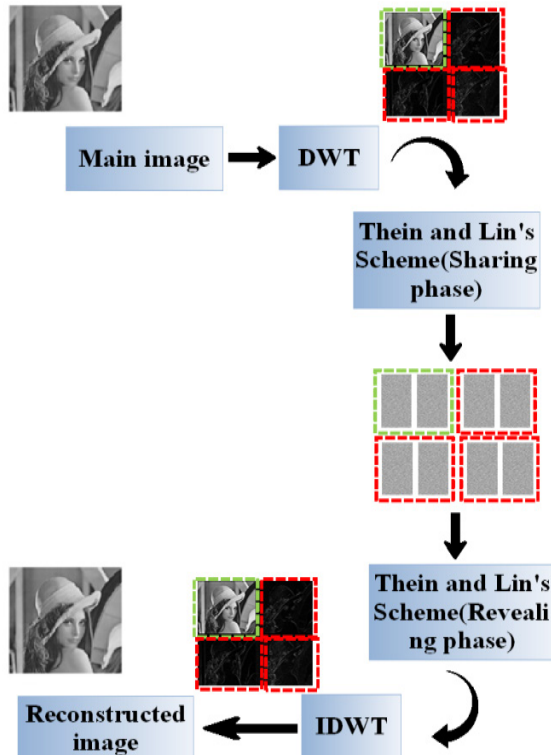

Figure 2. The proposed secret image sharing scheme

The proposed scheme is split into two procedures: sharing procedures and revealing procedures. In essence, the major advantage of the proposed scheme is that the size of each shadow is decreased with the increasing number of generated shares. Fig.2 illustrates the procedures of the partial image sharing.

3.1. Sharing Procedures

The sharing procedures can be described as follows:

- The secret image is passed through discrete wavelet transform.
- In this phase, the (T, N) threshold and the $(1-T)$ degree of sharing functions are firstly decided. The $(1-T)$ degree polynomial sharing function can be constructed by Eq. (1).
- Assume that T and N are determined so that a secret image I is shared by N shares $I_1, I_2, ..., I_N$. A number of T or higher is required to reveal secret image I by using Lagrange's interpolation formula. The pixel values $v_{sh_1}, v_{sh 2}, ..., v_{sh_N}$ for each share are obtained from Eq.(2).

$$v_{sh_1} = y(1), v_{sh 2} = y(2), ..., v_{sh_N} = y(N) \quad (2)$$

- The pixel values $v_{sh_1}, v_{sh_2}, ..., v_{sh_N}$ are separately assigned to N shares

3.2. Revealing Phase

The revealing phase can be described as follows:

- Suppose T shadows $I_1, I_2, ..., I_N$ are collected and pixels values $v_{sh_1}, v_{sh 2}, ..., v_{sh_N}$ are derived from the collected shadows so that sharing functions $y(1), y(2), ..., y(N)$ can be reconstructed by Lagrange's interpolation formula.
- We keep repeating step (1) until we process all the pixels in the share images.
- By completion step (2), we obtain the permuted image. Therefore, the inverse permutation has to be applied to obtain the compressed secret image.
- The inverse-discrete wavelet (IDWT) is applied on the resulted image to get the secret image.

For video encryption, our partial image secret sharing scheme is only applied on the I-frame because I-frame is the most significant frame in a Group Of Picture (GOP). Encrypting the I-frame is equivalent to encrypting the rest of the frames (i.e., P-frames) in the GOP. As a result, it would be impossible for an eavesdropper to obtain any information about the video sequence even if all the P-frames and B-frame are compromised. Here, we develop a video model to estimate the video quality of our proposed scheme. It is

known that the video quality can be estimated with different metrics such as Peak Signal-to-Noise Ratio (PSNR), the Structural Similarity index (SSIM), Moving Pictures Quality Metric (MPQM) and decodable frame rate (Q). In this paper, we use the decodable frame rate (Q) which is defined as the ratio between the numbers of successfully decoded frames to the total number of the frames sent.

$$Q = \frac{[N_{(dec-I)} + N_{(dec-P)} + N_{(dec-B)}]}{N_{(total-I)} + N_{(total-P)} + N_{(total-B)}} \quad (3)$$

Our model is based on secret sharing and it exploits the interdependency between the video frames in GOP. In the Moving Picture Experts Group (MPEG), GOP pattern is described by two parameters (N, M), where N defines the GOP length (i.e. the total number of frames within each GOP) and M is the number of B frames between I-P or P-P frames. For example as illustrated in Fig.3, (7,2) means that the GOP consists of one I-frame, two P-frames, and four B-frames. The second I-frame marks the beginning of the next GOP. The arrows indicate that the successful decoding of B and P-frames depends on the neighboring I or P-frames. The received packets usually suffer partial loss or total loss. Lost packets not only affect the frame to which they belong, but also they affect all the frames that have dependency on that frame. In other words, the error propagating from one frame to another, significantly degrade the quality of the whole video sequences.

Generally speaking, once the transmitter has a video sequence to be sent, every frame of the video sequence is split into a number of packets with size less or equal to the allowed maximum packet of the underlying network. The frames are reconstructed at the receiver if the number of decoded packet exceeds a threshold called the decodable threshold (*DT*). Table(1) shows the notation in this paper.

Table 1. Notations

Symbol	Stands for
N_{dec-I}	Expected number of decodable frames of I-frames
N_{dec-P}	Expected number of decodable frames of P- frame
N_{dec-B}	Expected number of decodable frames of B-frames
N_{GOP}	Total number of GOPs in the video stream
N_I, N_P, N_B	The number of packets in each type of frame
$N_{total-I}$	The total number of transmitted I-frames
$N_{total-P}$	The total number of transmitted P-frames
$N_{total-B}$	The total number of transmitted B-frames
p	Packet loss rate

In our proposed model, we made the following assumptions: (1) There is no error concealment techniques used at the decoder; (2) The packet loss rate is assumed to be constant during transmission. We assume independent and random packet loss p. The I-frame can be decoded successfully if its packets are delivered successfully. The probability that the I-frame packets are received at the decoder correctly is given by:

$$P_{dec-I}(I) = (1-p)^{N_I} \quad (4)$$

Then the expected number of correctly decoded I-frames for the entire video is:

$$N_{dec-I} = (1-p)^{N_I} N_{GOP} \quad (5)$$

A P-frame can be correctly decoded if the preceding I-frame and P-frames are correctly reconstructed The probability of decoding the first P-frame successfully is:

$$P_{dec-P}(P_1) = (1-p)^{N_I}(1-p)^{N_P} \quad (6)$$

The probability of decoding the second P-frame correctly is:

$$P_{dec-P}(P_2) = (1-p)^{N_I}(1-p)^{N_P}(1-p)^{N_P} \quad (7)$$

N_P represents the number of P-frames which in the case of GOP (N=7, M=2) is equal to 3. The expected number of successfully decoded P-frames for the whole video is calculated by:

$$N_{dec-P} = (1-p)^{N_I}\left(\sum_{j=1}^{N_P}(1-p)^{jN_P}\right)N_{GOP} \quad (8)$$

The B-frames can be correctly recovered if both the previous I-frame and next P-frame are decoded successfully and all the packets belonging to those B-frames are received correctly. The probability of decoding the first and the second group of B-frames is estimated by:

$$P_{dec-B}(B_1) = (1-p)^{N_I}(1-p)^{N_B} \quad (9)$$

$$P_{dec-B}(B_2) = (1-p)^{N_I}(1-p)^{2N_P}(1-p)^{N_B} \quad (10)$$

The last two group of B-frames can be decoded correctly if all the previous I, P-frames and the next I-frame in the next GOP are decoded successfully and all the packets belonging to those B-frames are received correctly.

$$P_{dec-B}\left(B_{\frac{N}{M}-1}\right) = (1-p)^{N_I}(1-p)^{N_P}(1-p)^{N_B} \quad (11)$$

$$P_{dec-B}\left(B_{\frac{N}{M}}\right) = (1-p)^{N_I}(1-p)^{2N_P}(1-p)^{N_B} \quad (12)$$

$$P_{dec-B} = \left[\left(1-p\right)^{N_I+N_{NP}N_P} + \sum_{j=1}^{N_P} \left(1-p\right)^{jN_P} \right] \cdot (M-1)\left(1-p\right)^{N_I+N_B} N_{GOP} \quad (13)$$

The expected number of successful decoded packets in B frames is:

By substituting (5), (8) and (13) into (3), the (Q) metric can be obtained. Here, Frames are secured unequally according to their importance. Therefore, only the I-frame is secured by using the proposed image secret method. Video quality could be improved by the secret shadows and the corresponding redundancy that resulting from increasing the number of shares which will be explained next.

The number of I-frames packets before employing the secret image sharing is N_I. After applying (T, N) secret sharing scheme, the number of I-frames is increased to:

$$N_{I_{new}} = N_I \left[1 + \frac{N-T}{T} \right] \quad (14)$$

We assume that the number of packets including the lost packets is $N_{I_{new}}$.

Then, the probability of receiving at least T packets from $N_{I_{new}}$ is

$$P_{dec-I}\left(I\right) = 1 - \sum_{i=T}^{N_{I_{new}}} \binom{N_{I_{new}}}{i} p_\beta^i \left(1-p_\beta\right)^{N_{I_{new}}-i} \quad (15)$$

Where $p_\beta = (1-p)^y$. It represents the probability of receiving y bits unharmed. Then the expected number of correctly decoded I-frames for the entire video is:

$$\begin{aligned} &P_{dec-I}\left(I\right) \\ &= 1 - \sum_{i=T}^{N_{I_{new}}} \binom{N_{I_{new}}}{i} p_\beta^i \left(1-p_\beta\right)^{N_{I_{new}}-i} \cdot N_{GOP} \end{aligned} \quad (16)$$

The expected number of successfully decoded P-frames is:

$$N_{dec-P} = \left(1-p\right)^{N_I} \left(\sum_{j=1}^{N_{NP}}\left(1-p\right)^{jN_I} \right) N_{GOP} \quad (17)$$

The expected number of successful decoded B-frames is:

$$N_{dec-B} = \left[\left(1-p\right)^{N_I+N_{NP}N_P} + \sum_{j=1}^{N_P} \left(1-p\right)^{jN_P} \right] \cdot (M-1)\left(1-p\right)^{N_I+N_B} N_{GOP} \quad (18)$$

By substituting (16), (17) and (18) into (2), the new (Q) metric can be obtained.

4. Experimental Results and Security Analysis

The performance of the proposed scheme is validated by the experiments. All the test images are taken from the USC-SIPI image database [14]. Two images 'Lena', 'Boat' with 512×512 pixels are used in the following experiments. These schemes have been implemented by Matlab. For the first experiment, Four and five shares from each band are produced by (2, 4) and (4, 5) respectively. The visual quality of the reconstructed images (i.e., PSNR value) are recorded. As we can see in the Fig.3 (a), the quality of the reconstructed image is excellent with very small loss due to the compression loss. We also compare the average PSNR of the new scheme and scheme of Thein and Lin's scheme [3]. Thresholds *(T=2, N=2)* and *(T=4, N= 4)* have been applied on Lena image and the generated shares are transmitted over a lossy channel. In the scheme, DWT is not applied and no redundant shares are sent over the erasure channel.
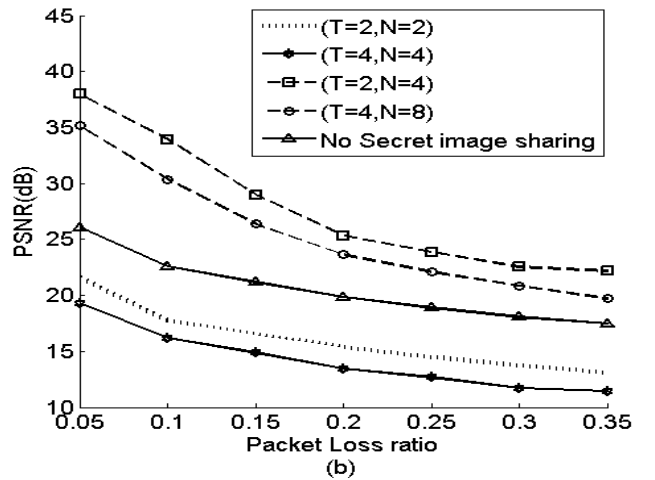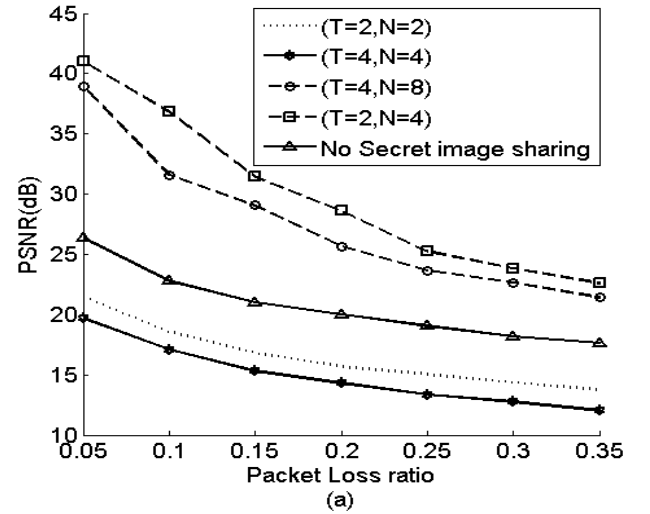

Figure 3. (a)Thein and method's scheme. (b) proposed scheme

The quality of the reconstructed image degrades as the number of threshold T increases as illustrated in Fig.3 (a).

The reason behind this is that losing one pixel of the share results in losing T pixels in the reconstructed image. Therefore, the schemes with higher thresholds degrade more sharply than the low threshold schemes. Share size in these experiments is $(128 \times 128) / T$.

In the third experiment, redundant shares have been transmitted to enhance reconstructed image quality. The schemes after adding redundant shares would be *(T=2, N=4)* and *(T=4, N=8),* respectively. The image quality has been improved as it is illustrate in Fig. 4(a). However, the redundant factor *(r)* for each one of these scheme is *2*. This means that the number of shares has been increased to twice its original number, which is quite high and not efficient if these schemes are employed in limited resource networks. In the last experiment, DWT divides the image into four bands, and each band with size $128 \times 128 / 4$. Redundant shares are only taken from the low frequency band.
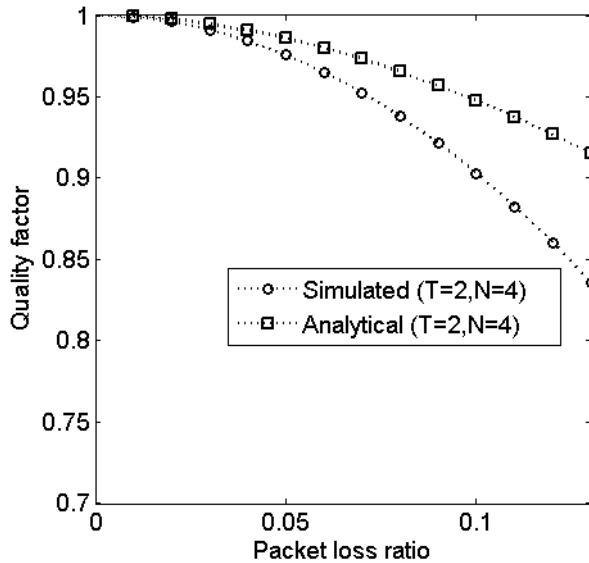

Figure 4.   Testing the proposed video metric

For *(T=2,N=4)* scheme, the redundancy factor r is equal to $r = ((64 \times 64 / 2) \times (4 + 6)) / (128 \times 128) = 1.25$. Thus, the redundancy factor has been reduced with *0.75* compared to Thein and Lin's scheme. Moreover, the proposed scheme gives PSNR close to Thein and Lin's scheme as illustrated in Fig.3 (b). The small difference in the reconstructed image between the two schemes happens due to DWT compression loss. A polynomial function with degree $1 - T$ requires at least T values to be reconstructed. In other words, at least any T shares are needed to reveal all sharing functions with the Lagrange interpolation formula. If an unauthorized user has $1 - T$ shares and desires to construct all sharing functions, there will be $(1/p)^n$, n stands for the number of sharing functions in all shares and p is the pixel value. To reconstruct a sharing function, an attacker must correctly estimate all coefficients for a sharing function. In our scheme, the probability of obtaining the correct coefficient in the sharing function is $(1/255)$ and that is only for one polynomial, but there are $(512 \times 512 / T)$ polynomials need to be solved for the coefficients. We have tested our analytical video quality metric for GOP (12, 3). It is observed from Fig.4 that analytical model performance is consistent with the simulation when the packet loss rate is slight. Then it diverges as the packet loss rate increases. The reason is that the analytical model does not consider error concealment at the decoder side while the simulation model includes error concealment technique. For small rate packet loss, there is no significant packet loss to be concealed so that both models provide close performance.

5. Conclusions

In this paper, we proposed a partial secret sharing scheme where the secret image is transformed by DWT into one low frequency band and three high frequency bands. Then Thein and Lin's scheme was applied in each band to generate shares. We investigated the issues of transmitting the shares over a lossy channel and proposed sending redundant shares of the low frequency band to mitigate the packet loss in the reconstructed image. Not just the proposed scheme succeeds in minimizing the redundancy significantly, but it also provides the same quality level as Thein and Lin's scheme. Our proposed partial image secret sharing can be utilized to secure the video transmissions.

ACKNOWLEDGEMENTS

REFERENCES

[1]   Shamir, "How to share a secret," *Communication of the ACM*, Vol. 22, no. 11, 1979, pp. 612-613.

[2]   L Bai, "A reliable (k, n) image secret sharing scheme with low information overhead,". Int. J. Compt. Appl. 32(1), 9–14 (2010).

[3]   R. Wang, Y. Lan, Y. Lee, SY Huang, S. Shyu, TL Chia, "Incrementing visual cryptography using random grids,". Opt. Commun 283, 4242–4249 (2010).

[4]   T. Chen, K. Tsao, "Threshold visual secret sharing by random grids,". *J. Syst. Softw 84*, 1197–1208 (2011).

[5]   C. N. Yang, K.H. Yu, and R. Lukac, "User-friendly image sharing in multimedia database using polynomials with different primes," *LNCS 4352, pp. 443-452, MMM 2007.*

[6]   S. Yamasaki, K. Matsushima, "A compression scheme of secret sharing," *Intelligent Signal Processing and Communications Systems (ISPACS), 2013 International Symposium on*, vol., no., pp.351,356, 12-15 Nov. 2013

[7]   W.-P.Fang, "Secret image sharing safety," *Communications, 2008. APCC 2008. 14th Asia-Pacific Conference on* , vol., no., pp.1-4, 14-16 Oct. 2008.

[8]   http://provideocoalition.com/sony/story/twice.

[9]   H. Koumaras, A. Kourtis, C.-H. Lin, and C.-K. Shieh, "A Theoretical Framework for End-to-End Video Quality Prediction of MPEG-based Sequences," *Networking and Services, 2007. ICNS. Third International Conference on* , vol., no., pp.62, 19-25 June 2007.

[10]   Z. Chen, Z. Xion, and L. Tang, "A novel scrambling scheme for digital video encryption," in *Proc. of Pac i fic-Rim Symposium on Image and Video Technology(PSIVT),* 2006, pp. 997-1006.

[11]   Z. Liu, X. Li, and Z. Dong, "Enhancing security of frequency domain video encryption," in *Proc. of ACM Multimedia,* 2004, pp. 304-307 2006, pp. 997-1006.

[12]   T. Chen, K. Tsao, "Threshold visual secret sharing by random grids,". *J. Syst. Softw* 84, 1197–1208 (2011).

[13]   Link: www1.icsi.berkeley.edu/PET/petapplications.html

[14]   Link: http://sipi.usc.edu/database/database.php?volume=misc

[15]   R. Brinkman, J. M. Doumen, and W. Jonker. Using secret sharing for searching in encrypted data. In *Workshop on Secure Data Management in a Connected World (SDM 2004),* volume 3178 of Lecture Notes in Computer Science, pages 18–27. Springer-Verlag, 2004.

[16]   L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," *in Proc. of ACM Multimedia*, pp. 219–229.

[17]   Sheng Cao, and Yong Chen, "Some secret sharing algorithms for Multimedia Security," *Computer Application and System Modeling (ICCASM), 2010 International Conference on* , vol.13, no., pp.V13-526-V13-529, 22-24 Oct. 2010.

[18]   W.W. Zhang*, Y.G. Wen, Z.Z. Chen and A. Khisti, "QoE-Driven Cache Management for HTTP Adaptive Bit Rate Streaming over Wireless Networks," *IEEE Transactions on Multimedia (TMM)*, Vol. 15, No. 6, October 2013, pp.1431-1445.

[19]   W.W. Zhang*, Y.G. Wen, K. Guan, D. Kilper, H.Y. Luo and D.P. Wu, "Energy-Efficient Mobile Cloud Computing under Stochastic Wireless Channel," *IEEE Transactions on Wireless Communications (TWC),* Vol. 12, No. 9, September 2013, pp. 4569-4581.

[20]   Y.G. Wen, X.Q. Zhu, J.P.C. Rodrigues and C.W. Chen, "Mobile Cloud Media: Reflections and Outlook (invited paper)," *IEEE Transactions on Multimedia (TMM)*, Vol. 16, No.4, June 2014, pp. 885-902.

[21]   Kejie Lu, Yi Qian, Mohsen Guizani, and Hsiao-Hwa Chen, "A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", *IEEE Transactions on Wireless Communications,* Vol.7, No.2, pp.639-647, February 2008.

[22]   Honggang Wang, Yi Qian, and Hamid Sharif, "Multimedia Communications over Cognitive Radio Networks for Smart Grid", *IEEE Wireless Communications*, Vol.20, No.4, pp.125-132, August 2013.

[23]   Liang Zhou, Rose Qingyang Hu, Yi Qian, and Hsiao-Hwa Chen, "Energy-Spectrum Efficiency Tradeoff for Video Streaming over Mobile Ad Hoc Networks", *IEEE Journal on Selected Areas in Communications,* Vol. 31, No. 5, pp.981-991, May 2013.