A NEW ERROR CONCEALMENT ALGORITHM UTILIZING THUMBNAIL IMAGES AND LSB DATA HIDING TECHNIQUE

Fatih Alagöz and Mohammed Abdel-Hafez

Department of Electrical Engineering
United Arab Emirates University
PO BOX. 17555, Al Ain, UAE.
Tel: +971 3 7051641, Fax: +971 3 7623156, E mail: {falagoz, mhafez}@uaeu.ac.ae

ABSTRACT

In this paper, we propose a new error concealment method for covering up the high packet losses of an original image after its transmission through an error prone-channel. In this method, we embed a number of thumbnail images of the original image into the same original image before the actual transmission. Unfortunately, most of the existing error-concealment techniques work only if the packet losses are smaller than a threshold and/or they are uniformly distributed. Utilizing thumbnail images and data hiding techniques is a potential approach to overcome this restriction. We investigate a modified Least Significant Bit (LSB) technique for embedding the thumbnails into the original image. Once the best thumbnail image is extracted from the recovered image subject to the channel conditions, we employ Spline Interpolation Technique (SIT) to estimate the lost macroblocks of the original image.

1. INTRODUCTION

Today's multimedia networks may not provide high fidelity for quality-of-service mechanisms due to many challenges such as packet dropping due to the congestion, packet lost due to bad channel conditions, intentional jamming, etc. [1]. In general, depending on the channel conditions and networks resources, FEC and/or ARQ schemes may be used for certain applications. As the new techniques yet to come, by making use of certain *a priori* knowledge about the multimedia data, *error concealment* technique has received particular attention as an effective mechanism to recover the packet losses in multimedia data without increasing the bandwidth demand [2,3]. In general, spatial, spectral, or temporal redundancies of the received multimedia data are utilized to perform error concealment [4]. Various interpolation approaches have been proposed each with a different tradeoff between the complexity and quality of multimedia data. For example, an edge directed interpolation technique may be used to improve the perceptual quality of recovered images by estimating the major edges in the corrupted blocks and by avoiding interpolation across the edges [5]. Unfortunately, error concealment mechanisms may suffer significantly from the packet losses that are larger than a threshold.

Besides improving the quality of the received multi-media content, today's multimedia networks also require a robust solution for copyright protection, since the duplication of multimedia data does not result in the inherent decrease in quality. One method of copyright protection for multimedia data is embedding a "watermark" into the original data [6-8]. This watermark is a digital code embedded in the multimedia data, which may typically indicate the copyright owner, any type of hidden data, etc. The watermark data may form a perceptual source itself, such as the application of audio in audio, image in image, video in video, data in data, and hybrid combinations. In general, the desired characteristics of digital watermarking can be listed as robustness, invisibility, security, low complexity, constant size, embedding capacity, etc. Excessive watermark size may harm the perceptual quality of the original multimedia data.

Error concealment and digital watermarking may be effectively combined for error concealment and recovery using data hiding techniques [9-11]. Particularly, some significant feature information is extracted from the original image and embedded back into the image itself. Then, this modified image with the hidden data is coded and transmitted over the network. At the receiver, the embedded data are reconstructed and the original image is restored based on the reconstructed hidden data along with some other post processing methods. Since some information of the lost data is hidden within the received packets, it is likely that error concealment may be conducted more successfully under help of the hidden data. For example, [9] conducts the data hiding in the block-DCT domain to protect the losses against JPEG compression. [10] performs interleaving during packetization to reduce the occurrence that adjacent blocks get corrupted simultaneously.

The motivation for this paper follows from the fact that the corrupted regions usually take the form of blocks or strips due to the block coding nature of the popular image/video codecs and the images/video packets transmitted through erroneous channel are subject to the loss of several macroblocks. Unfortunately, most of the

existing error-concealment techniques work only if the packet losses are smaller than a threshold and/or if the packet losses are distributed uniformly over the entire image [10]. The rest of this paper is organized as follows. Section 2 presents some background work for digital watermarking and the proposed error concealment algorithm. Section 3 presents the simulation results and discussions. Section 4 concludes this work.

2. THE PROPOSED ALGORITHM

2.1 Background in LSB Based Data Hiding

The simplest method of digital watermarking technique is to embed the watermark into the Least Significant Bits (LSB) of the cover image object [6]. Given the extraordinarily high channel capacity of using the entire cover for transmission, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark may be considered a success. However, despite its simplicity, the LSB technique brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. An even better attack may be engaged by simply setting the LSB bits of each pixel to one fully defeating the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark can be easily modified by an intermediate party.

A modified LSB technique that we implemented in our work uses a pseudo-random number generator to determine the pixels to be used for embedding based on a given key [6]. Security of the watermark may be improved, as the watermark is no longer easily viewed by intermediate parties. We note here that this algorithm, however, is still vulnerable to replacing the LSB's with a constant. Even in locations that were not used for watermarking bits, the impact of the substitution on the cover image is negligible. In general, the LSB modification proves to be a simple and fairly powerful tool for stenography at the expense of its low fidelity in secret communications. Since we expect no intentional attacks, for sake of its simplicity, we use the modified LSB technique for data hiding.

2.2 The Proposed Algorithm

We consider a scenario in which the upper part of the watermarked image is completely lost due to channel problems. Therefore, the received image is only the lower part of the watermarked image. By using the algorithm, we are able to recover the upper part of the image using the thumbnail images hidden in the lower part of the watermarked image. The proposed error concealment algorithm is as follows:

At the encoder:

i) Read in the original image with size of MxN pixels.
ii) Find the best performing thumbnail images each with size of $MxN/2^n$ pixels for $n = 0,1,2,3,...n_{max}$.
iii) Employ the modified LSB Data Hiding Technique to embed the thumbnails into the original image.
iv) Transmit the watermarked image via a two-state Gilbert channel.

At the decoder:

v) Receive the watermarked image.
vi) Employ LSB Data Extracting Technique to separate the original image and all the thumbnail images from the watermarked image.
vii) Using majority rule select the best thumbnail out of all the extracted thumbnail images.
viii) Estimate the lost macroblocks of original image using the best thumbnail.
ix) Write the recovered original image.

Figure 1 illustrates the instructive principles of the proposed algorithm.

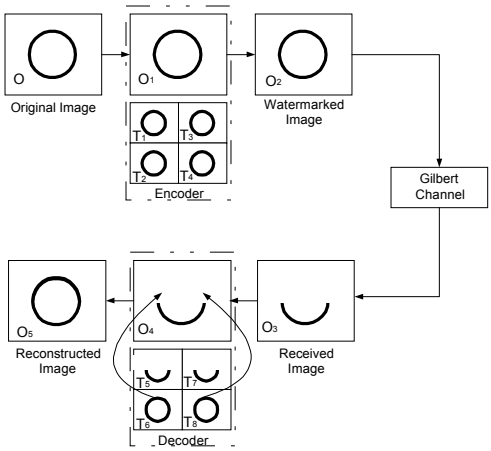

Figure 1. An illustration of the proposed algorithm.

In order to enhance the performance of the proposed algorithm, we consider the followings.

- The number and placement of thumbnail images to be embedded into the original image of size MxN pixels should be carefully studied. For the channel in consideration, we observed that the higher the thumbnail image size the better the image recovery due to providing better estimate in the course of resizing. Fortunately, in the modified LSB algorithm we may place the thumbnails over the entire image. We should note that the more data belonging to thumbnail images, the more perceptibility problems we experience. Other data embedding techniques may be explored to enhance perceptual quality.
- We consider the recovered thumbnail images should be used as a reference to recover the original images. As a simple approach, we only consider the majority rule based on Peak Signal-to-Noise Ratio (PSNR). Other exhaustive algorithms maybe developed to further improve the recovery. Since it is beyond the scope of this paper, we compare all the received thumbnail images and apply a simple decision rule to select the appropriate thumbnail to be used in the recovery of the original image.
- We consider two different estimation techniques for the lost macroblocks of the original image [12]. In

order to estimate the lost macroblocks of the original image we consider Nearest Neighbor Interpolation (NNI) and Spline Interpolation Technique (SIT) given in [12]. In the simulations, MATLAB Version 6.1 and ImageJ Version 1.29x [13] are used for the NNI and SIT techniques, respectively. One may consider other techniques such as a least-squared image resizing based on finite difference method, transform coding using inter-block correlation method, etc.

3. SIMULATIONS

3.1 Channel

The considered Gilbert channel operates based on a two-state Markov process. Packets belonging to an image are fully corrupted in the bad channel state while packet losses in the good channel states are negligibly small, i.e., packet loss of 10^{-4}. We assume that the packet losses are in consecutive orders based on the given transition probabilities. In the simulations, the channel starts with a bad state, and transition state probabilities are adjusted in way that 1%, 3%, 12%, 25% and 50% of the time the channel was in bad states. We note that due to the fading dynamics of an error-prone channel and/or the bottleneck at the transmitters, this scenario maybe highly expected for particular applications [1].

3.2. Simulation Results

We begin with a few notes on the results to follow. First, robustness evaluations were limited to testing against JPEG compression and the addition of random noise in bad channel states. Evaluating the algorithm against all attacks across a full range of gain values is beyond the scope of this paper. Since the primary use of this algorithm is to provide a new error concealment technique based on the LSB technique-using thumbnail images, the algorithm maybe exceptionally vulnerable to attacks. We are currently modifying the algorithm using more robust data hiding techniques.

For our reference image, the ever-popular miss November (Lena) image (384x384 pixels) is studied. Five different thumbnail watermarks were embedded into the original image; 6x6, 12x12, 24x24, 48x48 and 96x96 pixels. Figure 2. depicts the original image, a sample watermark image with 4-thumbnails each with 96x96 pixels. Figure 3. depicts the watermarked (transmitted) and received image subject to a packet lost of 50%. We note that the LSB method may support higher data hiding capacity at the expense of perceptual quality degradation.

The PSNR performance measurements is found based on the definition given in [6]

$$PSNR\,(dB) = 10\log_{10}\left\{\frac{XY\max\limits_{x,y} p_{x,y}^2}{\sum\limits_{x,y}\left(P_{x,y}-\overline{P}_{x,y}\right)^2}\right\} \qquad (1)$$

where X and Y are the same for 384x384 pixel Lena image at hand. P_{xy} and P'_{xy} denote the original image and measured image, respectively. Based on the PSNR definition given above and watermarked image with thumbnails sizes of 6x6, 12x12, 24x24, 48x8 and 96x96, the corresponding PSNR of watermarked images are 27.79, 27.29, 27.09, 27.37 and 26.99 dB, respectively.

Figure 2. a) Original image b)Watermark image

Figure 3. a) Watermarked image b)Received Image

Figure 4 and Figure 5 depict the recovered images using NNI and STI techniques, respectively, for different thumbnail sizes. Table 1 presents the corresponding PSNR measurements for each embedded thumbnail size and for different channel transition rates.

It is well known that the NNI technique is simpler to implement at the expense of blocky appearance. While the SIT technique is profoundly superior to the NNI technique for smaller thumbnail sizes, the gap between the two techniques gets smaller as the thumbnail image size increases. The first two columns of Table 1 suggests that regardless of the interpolation technique used, the best performing thumbnail size is achieved with the thumbnail image size of 96x96 pixels. This is due to the fact that the recovered thumbnail image carries more information about the original image. Since the considered channel is almost perfect channel during good states, we can extract the two of the thumbnails from the original received image. As we reduce the channel transition probability for bad channel state (from 50% to 25%, 12%, 3% and 1%, respectively) we observe that the use of the proposed algorithm vanishes. Although the PSNR measurements is superior to that of no watermark measurements, this superiority was not clear for the corresponding perceptual quality comparisons, especially at 3% and 1% bad channel conditions presented in the 5th and 6th columns of Table 1, respectively. This is due to the fact that the LSB data hiding employed in the proposed algorithm does not support the perceptual quality. Both human visual system and less imperceptible data hiding techniques maybe utilized to overcome the problems associated with perceptual analysis.

Figure 4. Recovered images based on the NNI technique for a) 24x24 (left) b) 96x96 pixels thumbnail images.

Figure 5. Recovered images based on the SIT technique for a) 24x24 (left) b) 96x96 pixels thumbnail images.

MxM	NNI (50%)	SIT (50%)	SIT (25%)	SIT (12%)	SIT (3%)	SIT (1%)
None	9.32	9.32	12.42	15.64	21.86	26.70
6x6	15.83	17.61	21.64	25.03	27.21	27.60
12x12	16.84	18.30	21.43	25.30	27.06	27.38
24x24	18.25	19.63	22.98	26.21	27.13	27.24
48x48	20.49	21.64	24.49	26.53	26.99	27.04
96x96	23.19	23.35	25.68	26.75	26.94	26.97

Table 1. PSNR (dB) measurements for each embedded thumbnail sizes and different channel conditions.

4. CONCLUSIONS

In this paper, we proposed a new error concealment method that is able recover the images subject to a transmission in an error prone-channel. For the embedding process, we use a modified Least Significant Bit (LSB) technique due to its simplicity. The LSB method may support higher data hiding capacity at the expense of perceptual quality degradation. In general, the size of hidden data should be much smaller than the size of original image so to provide imperceptibility as well as robustness. The Gilbert channel is represented by a two-state semi Markov process with good and bad states where the former acts almost as a perfect channel and the latter completely corrupts the transmitted packets. Unfortunately, most of the existing error-concealment techniques cannot cope with this type of channel conditions. Once the best thumbnail image is extracted from the recovered image subject to the above channel, we estimate the lost macroblocks of the original image using two types of interpolation techniques, namely, Nearest Neighbor Interpolation (NNI) and Spline Interpolation Technique (SIT). We show that the proposed error concealment technique is a simple yet promising one, especially for erroneous channels causing a wide range of packet losses. Since the target of this paper was to explore a new error concealment algorithm, we experienced imperceptibility problems due to the nature of the LSB technique. We are currently working on wavelet transform based data hiding technique for imperceptible watermarking.

5. REFERENCES

[1] F. Alagoz, et al, "Adaptive Rate Control and QoS Provisioning in Direct Broadcast Satellite Networks," *ACM Wireless Networks*, Vol. 7, No.3, pp.269-281, 2001.

[2] W. M. Lam and A. R. Reibman, "An Error Concealment Algorithm for Images Subject to Channel Errors," *IEEE Trans. on Image Processing*, vol. 4, no. 5, May 1995.

[3] Wang Y, Zhu Q-F, "Error Control and Concealment for Video Communication: A Review," *Proc. of IEEE,* vol.86, no.5, pp. 974–997, 1998.

[4] T. P. Chen and T. Chen, "Second-generation Error Concealment for Video Transport Over Error-prone Channels," *Wirel. Commun. Mob. Comput.,* vol. 2, 607–624, 2002.

[5] K. Jung, J. Chang, C. Lee, "Error Concealment Technique Using Projection Data for Block-based Image Coding," *Proc. of SPIE*, vol.2308, pp1466-1476, 1994.

[6] S.C. Katzenbeisser., et al "*Information Techniques for Steganography and Digital Watermarking*, Northwood, Artec House, 1999.

[7] M. Ramkumar, A.N. Akansu, "Information Theoretic Bounds for Data Hiding in Compressed Images," *Proc. IEEE Multimedia Signal Processing Workshop*, 1998.

[8] A.H. Tewfik, "Digital Watermarking," *IEEE Signal Processing Magazine*, vol 17, pp 17-88, September 2000.

[9] P. Yin, B. Liu, H. Yu: "Error Concealment Using Information Hiding," *Proc. of ICASSP'01*, 2001.

[10] M. Wu, "Multimedia Data Hiding," Ph.D. Thesis, Princeton University, 2001.

[11] M. Kurosaki, "Error Concealment Using Data Hiding Technique for MPEG Video", *IEICE Trans. Fundamentals*, Vol.E85-A, No.4, April 2002.

[12] P. Thevenaz, et al, "Image Interpolation and Resampling," Academic Press, New York, 2000.

[13] W.Rasband, "ImageJ 1.29X", National Institute of Health, USA. http://Rsb.info.nih.gov/ij, 2003.