IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 35-40

A Novel Data Hiding Scheme for High Dynamic Range Images

Punam wadekar[1] & Snehal Paliwal[2]
[1]M.Tech Student, [2]Assistant Professor
[1, 2] Electronic & Communication Engineering Department,
[1, 2] Tulsiramji Gaikwad Patil Collage of Engineering,
[1, 2] Rashtrasanta Tukdoji Maharaj Nagpur University, Nagpur, India
E-mail- [1]punamwadekar7@gmail.coml

Abstract: *In this paper, we propose a novel data hiding algorithm for high dynamic range (HDR) images encoded by the OpenEXR file format. The proposed algorithm exploits each of three 10-bit mantissa fields as an embedding unit in order to conceal k bits of a secret message using an optimal base which produces the least pixel variation. An aggressive bit encoding and decomposition scheme is recommended, which offers a high probability to convey (k+1) bits without increasing pixel variation caused by message concealment. In addition, we present a bit inversion embedding strategy to further increase the capacities.The generated stego HDR images and their tone-mapped low dynamic range (LDR) images reveal no perceptual differences when subjected to quantitative testing by Visual Difference Predictor.*

Keywords: *high dynamic range images, data hiding, OpenEXR, adaptive, optimal base, Visual Difference Predictor*

I. Introduction

A hiding, also known as data embedding, is a method of using digital media to conceal critical messages [1]. In general, the object in which secret messages are intended to be embedded is referred to as the cover medium, and the object in which the messages are concealed is called the stego medium. An image data hiding technique is usually evaluated in terms of the embedding capacity, also known as the payload, and the quality of the stego image communication. In recent years, interest in high dynamic range (HDR) images has increased dramatically [2] .The dynamic range of a scene is the contrast ratio between its brightest and darkest parts. allowing a far greater dynamic range of exposures than normal digital image techniques has been investigated herein. The first is the RGBE format [5], which adopts 32 bits per pixel to represent both luminance and chromatic information. The second is the uncompressed LogLuv TIFF format [6], which uses 48 bits for one pixel. The third is the OpenEXR format [7], which also employs 48 bits for a pixel to represent a dynamic range of luminance and chromatic information. Over the past few years, the OpenEXR format, developed by Industrial Light & Magic (ILM), has become an industry standard for HDR image formats due to its flexible and expandable structure. This format is considered the de facto standard in the movie industry [2] [8].The current state-of-the-art HDR watermarking works can be referred to in recent papers [11] [12]. Along with the wide availability of the distribution channels for providing applications such as video-on-demand and multimedia social networks, digital watermarking techniques aimed at preventing copyright violations for distribution channels have become more important than ever [19]. Unfortunately, research in HDR data hiding has not kept pace with advances made in HDR images, despite the fact that they provide great potential to become the leading image standard. To the best of the authors' knowledge, research into data hiding algorithms for HDR images has been very limited. These algorithms fall within two basic categories. The first type is intended to yield high capacity data hiding [13] [14]. This paper presents a novel data hiding algorithm using optimal base, abbreviated as DHOB, which employs an optimal base to conceal a serial secret bit stream with least distortion in a high dynamic range image encoded by 48-bit OpenEXR file format. This type of HDR image consists of three 16-bit floating-point values in the red, green and blue channels, all of them being "half" data types with 1-bit sign, 5-bit exponent and 10-bit mantissa field.

The proposed algorithm takes advantage of 10-bit mantissa fields to convey secret messages, while leaving intact the sign and exponent fields. When applicable, this scheme flips the secret bits before embedding, enabling the proposed aggressive bit encoding and decomposition scheme to carry extra payload for providing even higher embedding capacity. Considering a variety of luminance levels in an HDR image, we propose an adaptive data hiding scheme using optimal base, abbreviated as ADHOB, which supports luminance-aware message embedding, where more secret messages are carried on pixels with low luminance, and vice versa. This scheme exploits the feature of the human visual system since human beings are less sensitive to luminance variation when a pixel has low luminance. The experimental results using two image databases containing 30 OpenEXR images show that the proposed algorithm is flexible enough to offer high embedding capacity. The tone-mapped stego image shows a high image quality. The HDR visual difference predictor (HDR-VDP-2) test reveals a small probability of detection that the difference between the cover and the stego image is visible for an average observer. Our algorithm and its adaptive extension are not detectable under the LDR and HDR RS steganalytic attacks [19]. They can resist attacks from the LDR or HDR SPAM steganalyzers [20]. An intensive comparison shows that the proposed algorithm provides better performance than the current state-of-the-art competitors [13] . The major contribution of this work is in presenting the first data hiding algorithm in HDR images encoded by the OpenEXR format capable of providing a variety of capacities and producing high quality stego images feasible for real applications.

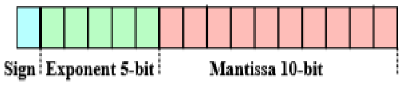


Fig. 1. The OpenEXR format represents pixel values using the "half" data type with 1-bit in the sign field, 5-bit in the exponent field, and 10-bit in the mantissa field in the red, green and blue channels.

A. An Overview of the OpenEXR Encoding

Format OpenEXR format or the Extended Range format recognized by the file name extension .exr is an open-source HDR image format developed by Industrial Light & Magic [2] [3] [4] [7] [8]. Starting in 1999, the format was developed for digital visual effects production, and the extended range format (.exr) was released as an open source C++ library in 2003. The bit breakdown for the OpenEXR half pixel encoding is shown in Fig. 1.

Their method provides an average embedding rate of 0.1355 bpp. Chang et al. [17] introduced a new distortion-free data embedding scheme for HDR images. They proposed a new homogeneity index table for homogeneity values of N=3, 5, 6, 7, which efficiently exploits all homogeneous representations of each pixel. Their scheme offers an average embedding rate of 0.1445 bpp. A survey of the literature indicates that there are three drawbacks in the current data hiding algorithm for HDR images.

Table I: The Abbreviations

Abbreviations	**Description**
ABCD	Aggressive bit encoding and
	decomposition scheme Adaptive data
ADHOB	hiding algorithm using optimal base
BIE	Bit inversion embedding technique
DHOB	Data hiding algorithm using optimal base
	Expected mean squared error High
EMSE	dynamic range
HDR	HDR visual difference predictor
HDR-VDP-2	Information content weighted structural
IW-SSIM	similarity measure
	Low dynamic range NMSE Normalized
LDR	mean squared error
	Optimal base
OB	Pearson's product-moment correlation
PPCC	coefficient
	PSNR Peak signal-to-noise ratio
PSNR	HDR image quality value
Q(H)	LDR image quality value
L((H)	Spearman's rank correlation coefficient
SSRC	Structural similarity index
SSIM	Visual saliency-based index
VSI	

This paper presents a novel data hiding algorithm for HDR images which is detailed in the next section.

II. Proposed Algorithm

This section describes the proposed DHOB algorithm. The scheme aims to conceal an extra bit for secret messages represented by a serial bit stream. This scheme decomposes the encoded decimal value into n message digits. We present an analysis of our algorithm in the final section. A. An Overview of the DHOB

Algorithm The flow chart of the message embedding in the proposed DHOB algorithm is shown in Fig. 2, which consists of three

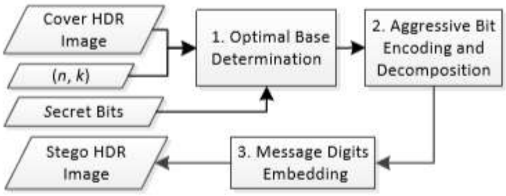


Fig. 2. Flowchart of embedding k secret bits into a pixel group of n pixels in the proposed DHOB algorithm.

processes. Given a pixel group of n pixels and the desired embedding bits k, the first process determines an optimal base (OB) which provides minimal pixel distortion for message concealment. The second process adopts the aggressive bit encoding and decomposition (ABED) scheme to produce n secret digits. The third process embeds these n secret digits into a pixel group of n pixels producing a stego HDR image. An aggressive bit encoding and decomposition scheme (ABED) is proposed, which offers a

A LIST OF VARIOUS CAPACITIES PROVIDED BY THE ABED SCHEME FOR THE GIVEN (N, K) AND THE DERIVED OPTIMAL BASE (OB)

n	k	$C_{\min}$	OB	T	C_{ABED}	Extra
3	4	1.3333	(2,3,3)	18	1.3750	510436
4	5	1.2500	(2,2,3,3)	36	1.2813	382827
5	8	1.6000	(3,3,3,3,4)	324	1.6531	650806
6	11	1.8333	(3,3,3,4,4,5)	2160	1.8424	111658
7	13	1.8571	(3,3,3,4,4,4,5)	8640	1.8650	85707
8	15	1.8750	(3,3,3,4,4,4,4,5)	34560	1.8818	83743
9	19	2.1111	(3,3,4,5,5,5,5,5,5)	562500	2.1192	99206
10	22	2.2000	(3,4,5,5,5,5,5,5,5,5)	4687500	2.2118	144050
11	25	2.2727	(4,5,5,5,5,5,5,5,5,5,5)	39062500	2.2877	182814

TABLE II

In this paper we use massage extraction for getting exact data whichever are hidden below given Formula to solve condition.

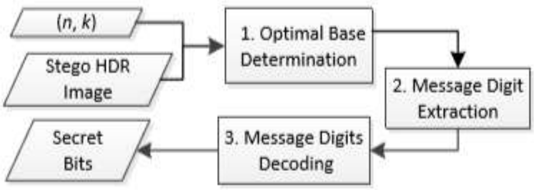
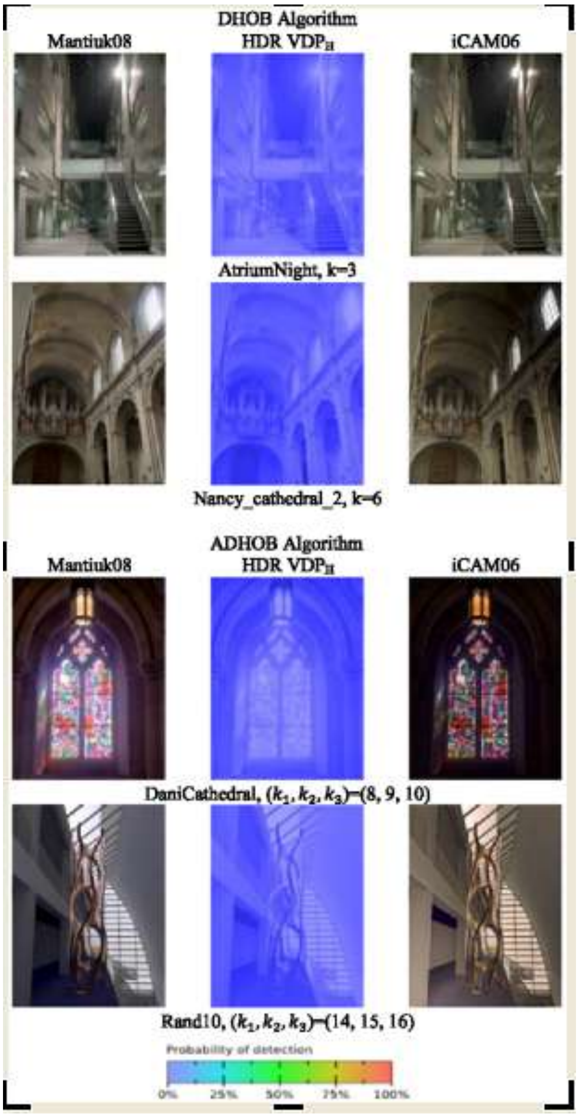


Fig. 3. Flowchart of message extraction in three processes

$$M_i' = \begin{cases} M_i & \text{if } v_i = 0 \\ M_i + v_i & \text{if } 0 < v_i < \lfloor b_i/2 \rfloor \\ M_i + v_i - b_i & \text{if } \lfloor b_i/2 \rfloor \le v_i < b_i. \end{cases} \quad (12)$$

The message extraction procedure operates in reverse. Note that since the exponent field is not altered during the message embedding, the exponent sorting and pixel classification produces the same {L1}, {L2} and {L3} in comparison to those conducted in the message embedding process

Colors seem to be more faithful when employing the TMO iCAM06.The experimental results are shown in Table III. This image show that the comparison between AHOB and DHOB algorithm which is provide information about hidden data acknowledgement process. with the OpenEXR pixel encoding format, no suspicion is raised when checking the legality of the he HDR encoding format. Nevertheless, concealing secret messages in the mantissa field is similar to adopting the least significant bit substitution approach in the LDR image. TableIII shows the results of the HDR RS steganalysis. The statistics reveal more or less the similar range of values for RM, R-M, SM and S-M. In addition, there is a small absolute difference for DIR and DIS in three channels using either DHOB or ADHOB algorithms.



The experimental results are shown in Table III

TABLE III

Consequently, the stego images generated by our ADHOB algorithms are also undetectable by the SPAM steganalyzer is unable to directly detect stego HDR images produced by the ADHOB algorithm. The steganalytic statistics indicate that our proposed DHOB and ADHOB algorithms are secure against the LDR RS, HDR RS, LDR SPAM and HDR SPAM steganalysis.

The comparison shows that our algorithms demonstrate the most effective data hiding method. With regard to the image quality, our scheme produces the highest PSNR, lowest normalized mean squared error (NMSE) and largest range of PPCC and SRCC, which is close to 1.0. The experiment shows that the message embedding or extraction occupies one-tenth of the execution time, while most of the time is spent in processing the input/out and constructing the dynamic data structures for message concealment. Not surprisingly, it takes a longer time for our algorithm to conceal and extract secret messages when using a larger image resolution for testing. The comparison shows that our algorithm provides the best performance, outperforming the current state-of-the-art methods.

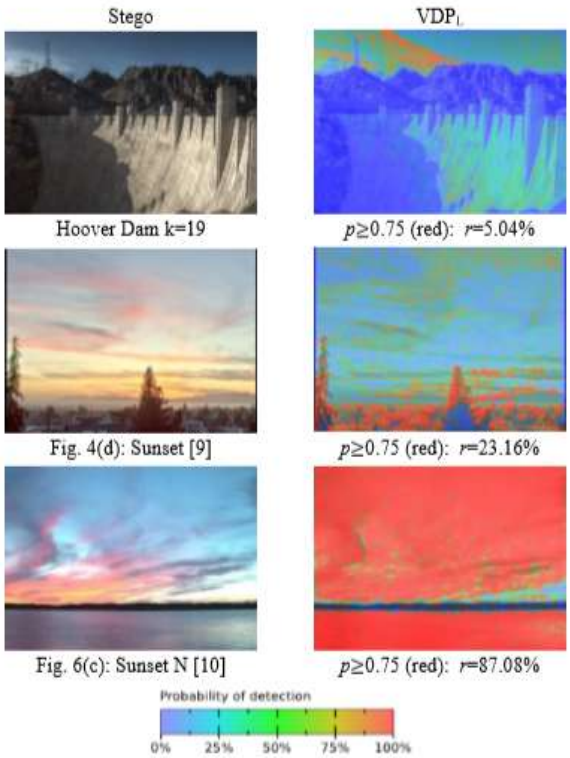


Fig.7. The VDP-2 comparison for results produced by our algorithm, Wang and Cheng's, and Li et al.'s works

Fig. 7 shows the HDR-VDP-2 comparison results for Wang and Cheng's algorithm, Li et al.'s method and our DHOB algorithm. Detailed statistics and images with a larger resolution are shown in the supplemental material F. Our algorithm reveals the ratio of pixels r=5.04% for the probability of detection p>0.75, where pixels shown with red represent the probability of detection map p>0.75. A small r for p>0.75 indicates low visual image differences between the cover and stego images. In contrast, the best result is r=23.16% for Wang and Cheng's algorithm and r=87.08% for Li et al.'s method, both under the condition for p>0.75. In addition, our algorithm produces a high Q(L) value over 63.01. The comparison shows that our algorithm outperforms the current state-of-the-art methods.

III. Conclusions And Future Work

This paper presents a novel data hiding algorithm for HDR images encoded by the OpenEXR format. The proposed algorithm conceals secret messages in the 10-bit mantissa field in each pixel, while the 1-bit sign and 5-bit exponent fields are kept intact. We recommend an optimal base allowing secret messages to be concealed with the least pixel distortion. An aggressive bit encoding and decomposition scheme is introduced herein, which offers the benefit for concealing an extra bit in a pixel group without incurring pixel distortion. The influence of the message probability is analyzed, and the embedding capacity is further increased by taking advantage of the recommended bit inversion embedding scheme. The analysis indicates that the proposed algorithm can resist attacks from the LDR and HDR RS steganalyzer and the LDR and HDR SPAM steganalysis. The contribution of this work is in presenting the first data hiding algorithm for OpenEXR HDR images. The proposed algorithm provides a high embedding capacity, which makes use of an aggressive bit encoding and decomposition scheme, as well as the bit inversion technique. Our scheme produces a stego image with high quality, taking advantage of the optimal bases to produce the least pixel distortion

Appendix A

We prove in this section that (3) represents the expected mean squared error for an optimal base b. Without loss of generality, let M represent the mantissa part of a pixel and r=M mod b = 0. Referring to (12), when b is an even integer (b≥2), we can conceal secret digits v=0, 1, …, $b/2$, $(b/2)+1$…, b-1 and produce the stego mantissa M'=M, M+1, …, M+$b/2$, M-$(b/2-1)$, .., M-1. Thus, we can derive $EMSE(b)$ in (A-1). When 1≤r≤(b-1), we produce the same result because of the commutative law of addition

$EMSE(b) =$
$\{02+12+\cdots+(b2)2+[-(b\ 2-1)]\ 2+\cdots+(-1)2\}$
$\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$
b

$= \frac{b2+2}{12}$ (A-1)

We now consider the case when b is an odd integer (b≥1). Referring to (12), we can conceal secret digits v=0, 1, …, (b-1)/2, (b-1)/2+1, …, b-1 and produce the stego mantissa M'=M, M+1, …, M+(b-1)/2, M-(b-1)/2, …, M-1. We can derive $EMSE(b)$ in (A-2). When 1≤r≤(b-1), we produce the same result.

$EMSE(b) =$ $\{02+12+\cdots+[b-1\ 2\ ]\ 2+[-(b-1\ 2\ )]2$
$+\cdots+(-1)2\}$
$\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$
b
$= b2-1/\ 12$ (A-2)

$EMSE(b) =$ $b2-(-2)[(b+1)\mathrm{mod}\ 2]/\ 12$
(A-3)

Acknowledgment

This work was supported in part by a grant from the National Science Foundation Contribution of collage professor who might have given me suggestions for completion paper.

References

[1]. D. Artz, “Digital steganography: Hiding data within data,” IEEE Internet Comput., vol. 5, no. 3, pp. 75–80, May/Jun. 2001.
[2]. F. Banterle, A. Artusi, K. Debattista, and A. Chalmers, Advanced high dynamic range imaging: theory and practice, AK Peters Ltd., Natick MA, 2011, pp. 22–26.
[3]. E. Reinhard G. Ward, S. Pattanaik, P. Debevec, W. Heidrich and K. Myazkowski, High dynamic range imaging: acquisition, display, and image-based lighting, 2nd ed., Morgan Kaufmann, 2010, pp. 103–104.
[4]. B. Hoefflinger, High-dynamic-range (HDR) vision, microelectronics, image processing, computer graphics, Springer, 2007, pp. 181–183.
[5]. G. J. Ward, “The RADIANCE lighting simulation and rendering system,” Computer Graphics (Proceedings of ’94 SIGGRAPH conf.), pp. 459–72, Jul. 1994
[6]. G. W. Larson, “LogLuv encoding for full-gamut, high-dynamic range images,” Journal of Graphics Tools, vol. 3, no. 1, pp. 15–31, 1998.
[7]. Industrial Light & Magic, OpenEXR, http://www.openexr.com/downloads.html, 2015.
[8]. R. Fernando, GPU gems: programming techniques, tips and tricks for real-time graphics, Addison-Wesley, 2004, Chapter 26. [Online]. Available: https://developer.nvidia.com/gpugems/GPUGems/gpugems_ch26.html
[9]. Z. Qian, X. Zhang, and Z. Wang, “Reversible data hiding in encrypted jpeg bitstream,” IEEE Trans. Multimedia, vol. 16, iss. 5, pp. 1486– 1491, 2014.
[10]. M. S. Subhedar and V. H. Mankar, “Current status and key issues in image steganography: a survey,” Computer Science Review, vol. 13-14, pp. 95–113, Nov. 2014.
[11]. E. Maiorana and P. Campisi, “High-capacity watermarking of high dynamic range images,” EURASIP J. on Image and Video Process. 2016, 2016:3, doi:10.1186/s13640-015-0100-7, 2016.
[12]. E. Maiorana and P. Campisi, “Multi-bit watermarking of high dynamic range images based on perceptual models,” Security and Comm. Networks, doi: 10.1002/sec. 1345, 2015.
[13]. Y. M. Cheng and C. M. Wang, “A novel approach to steganography in high-dynamic-range images,” IEEE Multimedia, vol. 16, no. 3, pp. 70– 80, Jul.-Sept. 2009.
[14]. M. T. Li, N. C. Huang, and C. M. Wang, “A data hiding scheme for high dynamic range images,” Int. J. of Innovative Computing, Inf. and Control, vol. 7, no. 5, pp. 2021–2035, May 2011.
[15]. C. M. Yu, K. C. Wu, and C. M Wang, “A distortion-free data hiding scheme for high dynamic range images,” Displays, vol. 32, no. 1, pp. 225–236, 2011.
[16]. C. C. Chang, T. S. Nguyen, and C. C. Lin, “Distortion-free data embedding scheme for high dynamic range images,” J. of Electronic Science Technology, vol. 11, no. 1, pp. 26–26, 2013.
[17]. C. C. Chang, T. S. Nguyen, and C. C. Lin, “A new distortion-free data embedding scheme for high-dynamic range images,” Multimedia Tools and Applications, Sep. 2014 (DOI 10.1007/s11042-014-2279-5).
[18]. Z. H. Wang, C. C. Chang T. Y. Lin, and C. C. Lin, “A novel distortion-free data hiding scheme for high dynamic range images,” in Proc. Of the 2012 Fourth Int. Conf. on Digital Home, pp. 33–38, Guangzhou, Nov. 23-25, 2012.
[19]. J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color and gray-scale images,” IEEE Multimedia, vol. 8, no. 4, pp. 22– 28, Oct./Dec. 2001.
[20]. T. Pevný, P. Bas, and J. Fridrich, “Steganalysis by subtractive pixel adjacency matrix,” IEEE Trans Inf. Forensics Security, vol. 5, no. 2, pp. 215–224, June 2010.
[21]. C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition, vol. 37, no. 3, pp. 469-474, Mar. 2004. and J. J. Liou, “Pseudo-multiple-exposure-based tone fusion with local region adjustment,” IEEE Trans. Multimedia, vol. 17, no. 4, pp. 470– 484, Apr., 2015.