International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

A Novel Data Hiding Scheme for High Dynamic Range Images

Punam wadekar[1] & Nagma Sheikh[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* , [2]*nagma.ece@tgpcet.com*

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 when the probability of appearance of secret bit "1" is greater than 0.5. Furthermore, we introduce an adaptive data hiding approach for concealing more secret messages in pixels with low luminance, exploiting the features of the human visual system to achieve luminance-aware adaptive data hiding. The stego HDR images produced by our algorithm coincide with the high dynamic range image file format, causing no suspicion from malicious eavesdroppers. 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. Our algorithm can resist steganalytic attacks from the HDR and LDR RS and SPAM steganalyzers. We present the first data hiding algorithm for OpenEXR HDR images offering a high embedding rate and producing high visual quality of the stego images. Our algorithm outperforms the current state-of-the-art works.

Keywords

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

1. 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. On one hand, data hiding algorithms should maximize the quantity of messages that can be conveyed. Offering a large payload plays an important role for applications such as the annotation of images. On the other hand, the data hiding algorithms should minimize the embedding distortion, producing a high quality stego image to resist steganalytic attacks, which attempt to detect the presence of hidden messages. A data hiding algorithm which can provide a plausible stego image with a sufficient and secure payload raises no suspicion to a malicious eavesdropper and thus is suitable for applications such as covert communication. In recent years, interest in high dynamic range (HDR) images has increased dramatically [2] [3] [4]. The dynamic range of a scene is the contrast ratio between its brightest and darkest parts. HDR images represent a large range of luminance using floating-point numbers. This is in contrast to low dynamic range (LDR) images which represent a limited range of luminance using integers. A set of advanced image techniques allowing a far greater dynamic range of exposures than normal digital image techniques has been investigated herein. The scenario behind these

techniques involves accurately representing the wide range of intensity levels found in real scenes, ranging from direct sunlight to deepest shadows, in order to exhibit the accurate fidelity of a real scene. There are three main HDR image formats. 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]. For example, it was adopted by Hollywood film editors and special effects directors to produce the film Harry Potter and the Sorcerer's Stone. The OpenEXR format covers the entire visible color gamut and the full range of perceivable luminance, thus providing optimal visual fidelity on a variety of output devices. Because of their great potential, HDR images encoded by the OpenEXR format are expected to replace LDR images, and will serve as one of the new image standards in the future. A number of data hiding algorithms have adopted LDR images, such as binary, grayscale, or color images, to conceal secret messages [9] [10]. Watermarking algorithms, which emerged as an enabling technology to protect the intellectual property of digital contents, were investigated for HDR images [11]-[18]. The current state-of-the-art HDR watermarking works can be referred to in recent papers [11] [12] [17]. 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 [20] [21]. These algorithms convey a large amount of secret messages at the cost of producing a stego image with large distortion. They are current state-of-the-art algorithms, providing an embedding rate of at least 5 bits per pixel. The second type of algorithm is intended to yield high image quality of data hiding [22] [23] [24] [25]. These algorithms specifically exploit the RGBE HDR encoding format to conceal a small quantity of messages; unfortunately, the capacity offered by these algorithms is limited to less than 0.5 bits per pixel. They are also referred to as distortion-free algorithms because any distortion produced after the secret message embedding is so insignificant that the stego image generated after the tone-mapping operation is identical to the cover tone-mapped image. Since the capacity offered by these distortion-free algorithms is limited, it becomes difficult for them to support applications that require large capacity. Developing an HDR data hiding algorithm is a distinct challenge. Unlike the fixed range of luminance for an LDR image, each HDR image has a very different luminance range. An HDR data hiding algorithm must cope with a different luminance range that provides high capability while keeping the distortion of the stego image as small as possible. In addition, the encoding format of the stego HDR image should be coincident with the original HDR image, arousing no suspicion from malicious eavesdroppers. Finally, when a cover and stego image are tone mapped for the purpose of visualization, the image quality should be visually plausible, and the difference between them should not be visible to a human observer. 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. The main idea behind our algorithm is to derive an optimal base (OB) to decompose k secret bits into n secret digits in an M-ary notational system, where M is determined by the derived optimal base. Using an optimal base ensures that a stego image can be produced with the least image distortion when concealing these secret M-ary digits. In addition, we introduce an aggressive bit encoding and decomposition (ABED) scheme which offers a high probability to convey (k+1) bits rather than k secret bits, thereby providing a higher embedding capacity without increasing the pixel variation. We analyze the probability of message appearance and recommend a bit inversion embedding (BIE) scheme. 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 [26]. They can resist attacks from the LDR or HDR SPAM steganalyzers [27]. An intensive comparison shows that the proposed algorithm provides better performance than the current state-of-the-art competitors [20] [21]. 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. This paper is organized as follows. Related works are reviewed in Section II, and the proposed algorithm is presented in Section III. The experimental results and comparisons are detailed in Section IV. Section V offers conclusions and possible future work. Detailed experimental statistics are presented in the supplemental materials A-H.

II. RELATED WORK This section surveys data hiding approaches for HDR images. First, a brief description of the OpenEXR encoding format is given, and then data hiding algorithms proposed in the literature are described.

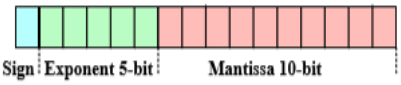


Fig. 1. The OpenEXR format represents pixel values using the "half" data type with 1-bit in the sign field, 5-bit in the exponent field, and 10-bit in the mantissa field in the red, green and blue channels.

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. Each color is encoded using a half precision floating point number, which is a 16-bit implementation of the IEEE 754 standard. The formula of a pixel P converted from an encoded value is shown in (1), where SN represents the 1-bit sign, E indicates the 5-bit exponent and M denotes the 10-bit mantissa. Thus, the format is also known as S5E10. Note that when E=0 and M2 > 0, the value being represented is a subnormal number; when E is in the range of 1 and 30, a hidden one always exists to increase the representation precision. In addition, when E=31, the represented value is either a positive or negative infinity if M2=0 or not a number (NaN) if M2 > 0.

$$P = \begin{cases} 0 & \text{if } (E = 0 \,\&\, M = 0) \\ (-1)^{SN} 2^{-14} (0.M_2) & \text{if } (E = 0 \,\&\, M > 0) \\ (-1)^{SN} 2^{E-15} (1.M_2) & \text{if } (1 \le E \le 30) \\ \pm\infty & \text{if } (E = 31 \,\&\, M = 0) \\ NaN & \text{if } (E = 31 \,\&\, M > 0). \end{cases} \quad (1)$$

The interpretation of the sign, exponent and mantissa is analogous to IEEE-754 floating-point numbers. The final format is 48 bits, covering around 10.7 orders of magnitude. The range of representative numbers is roughly 5.96×10-8 to 65504. One of the main advantages of OpenEXR encoding is that this format is implemented in graphics hardware, e.g., supported natively by the NVIDIA 3D GeForce FX graphics solutions allowing real-time applications for HDR images [4] [8]. Other advantages include that this format can be used by multiple lossless image compression algorithms, and it supports flexible extensibility to include new compression codes, image types and image attributes [4].

B. A Survey of Data Hiding Algorithms

for HDR We examined several data hiding algorithms for HDR in the literature, focusing on algorithms which provide high embedding capacity, followed by those offering high quality of images. Cheng and Wang [20] pioneered in presenting an adaptive steganographic algorithm with authentication for an HDR image encoded by the RGBE format developed for radiance software [5]. The range of luminance intensity is decided by the 8-bit exponent field (E) for all three color values in each pixel. Their algorithm took advantage of this to classify pixels into flat or boundary areas in order to convey different quantities of

secret messages, thus achieving adaptive message embedding. They employed a two-sided approach which considers an input pixel and its two neighboring pixels (upper and left) in order to estimate the number of adaptive bits to be embedded on this input pixel. This two-sided approach was

extended to become an L-sided approach which considers three neighboring pixels (upper, left and upper-left), thereby offering a more accurate estimation. Their algorithm adopted a pixel as an embedding unit and provided an embedding rate in the range of 5.13 to 9.69 bits per pixel (bpp). The peak signal-to-noise ratio (PSNR) values for the tone-mapped stego images are only slightly greater than the 30 dB which are acceptable to human perception. Li et al. [21] proposed a data hiding scheme for HDR images which improves the embedding capacity of Cheng and Wang's scheme. Instead of using HDR images encoded in 32-bit radiance RGBE coding, Li et al. used an HDR image encoded by a 48-bit TIFF format, where each channel has 16 bits, including a 1-bit sign field, a 5-bit exponent field, and a 10-bit mantissa field. The secret messages are embedded into the mantissa field, leaving the sign and exponent fields intact. Based on the optimal pixel adjustment process (OPAP) [28], they introduced three data hiding strategies which offer an exquisite balance between high embedding capacity and the quality of the tone-mapped stego images. Their algorithm adopted a pixel as an embedding unit and provided an average embedding rate of 26 bpps. The tone-mapped stego image has a PSNR value in the range of 30.47-37.00 dB. Li et al.'s algorithm outperforms Cheng and Wang's method in the embedding rate. Several data hiding algorithms presented in the literature offer a low distortion manner of message concealment and produce a high image quality. All of them focus on the radiance RGBE format. Yu et al. [22] presented the first low distortion data hiding algorithm for HDR images. They observed that the exponent channel demonstrates more than one homogeneous representation. Thus, their scheme takes advantage of encoding secret messages to a pixel's homogeneous representations, thus producing a tone-mapped stego image that is identical to the tone-mapped cover image. For the application of HDR image annotation, the average embedding rate offered by their method, using an image database with 125 HDR images, is in the range of 0.12-0.29 bpp. However, an average embedding rate is reduced to the range of 0.0010-0.0026 bpp for the application of image steganography because their algorithm exploits a small number of pixels to conceal secret messages so that the stego image complies with the radiance RGBE encoding format, remaining undetectable to malicious eavesdroppers. Wang et al. [25] introduced a segment-based data hiding scheme for HDR images encoded by the radiance RGBE format. A number of non-overlapping G pixels in the cover HDR image are grouped together to form a segment. In every segment, each pixel's homogeneous representations are multiplied together, offering even more homogeneous representations. This allows their algorithm to exploit Yu et al.'s approach of concealing more secret bits. Given G=1000, the average embedding rate is in the range of 0.135-0.140 bpp. Chang et al. [23] proposed a distortion-free data embedding scheme for HDR images. Their scheme takes advantage of the Cartesian product of all of the HDR pixels, thus exploiting all

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
EMSE	Expected mean squared error High
HDR	dynamic range
HDR-VDP-2	HDR visual difference predictor
IW-SSIM	Information content weighted structural similarity measure
LDR	Low dynamic range NMSE Normalized mean squared error
OB	Optimal base
PPCC	Pearson's product-moment correlation coefficient
PSNR	PSNR Peak signal-to-noise ratio
Q(H)	HDR image quality value
L((H)	LDR image quality value
SSRC	Spearman's rank correlation coefficient
SSIM	Structural similarity index
VSI	Visual saliency-based index

of the homogeneous representations. Their method provides an average embedding rate of 0.1355 bpp. Chang et al. [24] 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. First, while most algorithms target the 32-bit radiance RGBE or 48-bit TIFF format, none of them is developed for the OpenEXR format. Second, while works reported by [23] [24] [25] constantly increase the embedding capacity, a stego HDR image generated by these algorithms does not preserve the radiance RGBE encoding format, thus becoming perceptible to eavesdroppers and vulnerable to steganalytic attack. Third, most algorithms do not consider how to

minimize pixel distortion incurred from message concealment, thus producing a tone-mapped stego image with a moderate image quality. This paper presents a novel data hiding algorithm for HDR images which is detailed in the next section.

III. PROPOSED ALGORITHM This section describes the proposed DHOB algorithm. We list the abbreviations in Table I for quick reference. First, we highlight an overview of the algorithm in terms of the message embedding, and then describe the optimal base, a kernel concept of the algorithm, followed by the proposed aggressive bit encoding and decomposition scheme (ABED). 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. Next, the approach of embedding and extracting these n message digits is described. Furthermore, we describe an extension of the proposed algorithm to support luminance-aware adaptive data hiding. 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

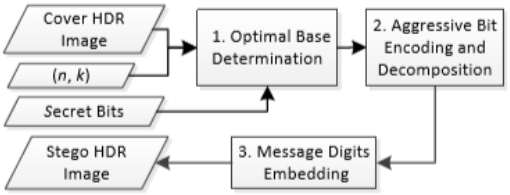


Fig. 2. Flowchart of embedding k secret bits into a pixel group of n pixels in the proposed DHOB algorithm.

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. B. The Concept of the Optimal Base A fundamental requirement of a message embedding algorithm is to satisfy various desirable capacities. The input of the DEOB algorithm is (n, k) which indicates that k secret bits are concealed in a pixel group of n pixels, offering the capacity of k/n bits per pixel. The proposed algorithm can thus provide a variety of capacities by altering n and k. We conceal secret messages through the use of the optimal base. Two examples, n=1 and n=3, are given before a formal definition for the optimal base is provided. Without loss of generality, take (n, k)=(1, 2) as an example; this conceals 2 secret bits in a single pixel P providing an embedding rate of 2.0 bpp. Take a base b=4≥22, which provides four pixel change patterns to convey four decimal secret messages 0, 1, 2 or 3, since k=2. For example, if P mod b = 0, the four pixel change patterns P+0, P+1, P+2, P-1 can convey secret messages 0, 1, 2 or 3, respectively, and the pixel distortion expressed in terms of the expected mean squared error (EMSE) has the smallest value of [02+12+22+(-1)2]/4=1.5, assuming secret messages have equal probability of appearance. Similarly, if P mod b = 1, 2 or 3, secret messages can still be concealed by four pixel change patterns using different orders, producing the same mean squared errors of 1.5. In this example, b=4 is an optimal base because it offers the requested embedding rate ($\lfloor log 24 \rfloor$ bpp) and produces the least expected mean squared error, 1.5. A more general case is considered by taking an optimal base b which provides b number of pixel change patterns to conceal secret messages 0, 1, …, b-1. The capacity offered by the optimal base b is shown in (2), and the expected mean squared error produced is shown in (3). The proof is detailed in Appendix A. Note that if b=2k, the capacity and the distortion provided equals the well-known OPAP message embedding scheme. In other words, OPAP is a special case of employing an optimal base b=2k:

$$C(b)=\lfloor log 2b \rfloor. \quad (2)$$

$$EMSE(b) = [b2 -(-2)[(b+1) mod\ 2]]/12. \quad (3)$$

Now consider the second example of n=3. Without loss of generality, take (n, k)=(3, 4) as an example which conceals 4

secret bits in a pixel group of 3 pixels. Since k=4, the secret messages are decimal values from 0 to 15. Without loss of generality, assume OB=(b1, b2, b3) is an optimal base, where $b1 \leq b2 \leq b3$. Based on the first example, OB must satisfy the first inequality, b1×b2×b3≥24, in order to satisfy the requested embedding rate, 4/3 bpp. In addition, OB must produce the least expected mean squared error, min[∑ EMSE(bi) 3 i=1]/3, when concealing secret messages. It is possible to approximate the first inequality using the inequality of arithmetic and geometric means (AM-GM inequality). In particular, when b1=b2=b3=√24 3 ≈2.5198, the equality b1×b2×b3=24 holds. Since bi is an integer, we derive the lower bound of bi using the floor function ⌊√24 3 ⌋ = 2 and the upper bound of bi using the ceiling function with a slightly larger range ⌈√24 3 ⌉+1=4. This indicates bi ∈{2, 3, 4}; there are a total of 33 possible optimal bases, including (2, 2, 2), (2, 2, 3), …, (4, 4, 4). Consequently, the optimal base OB=(2, 3, 3) is derived, where the embedding rate offered by this optimal base is $\lfloor log 2(b1 \times b2 \times b3) \rfloor/3$ =1.3333

bpp, satisfying the requested rate. In addition, the OB produces the smallest expected mean squared error, EMSE(2, 3, 3)=0.6111. Note that if $b1 \le b2 \le b3$is not restricted, then (3!/2!) optimal bases will be derived, including OB=(2, 3, 3,), (3, 2, 3) and (3, 3, 2). The two examples are now generalized by considering that the secret message is carried by a pixel group (PG) of n pixels, PG(P1, P2, …, Pn). Referring to the examples, given (n, k), an optimal base $OB = (b1,b2,\ldots,bn)$ must satisfy the first inequality shown in (4) in order to provide $2k$ pixel change patterns satisfying the requested embedding rate (k/n) bpp. Besides, the OB must produce the least pixel distortion, as shown in (5). We approximate the first inequality by finding the lower and upper bounds of each vector component (bi), as shown in (6). Then, we derive an optimal base from a total of $3n$ possible optimal bases. Equation (7) expresses the minimal embedding rate offered by OB in bpp, where $T = \prod bi\ n\ i$=1 is called the maximal pixel change patterns and the expected mean squared error produced by OB is shown in (8).

$$T=\prod bini=1\geq 2k \quad .(4)$$

$$OB =(b1,b2,\ldots,bn) =arg\ \min\{\sum \mathrm{EMSE}(bi)/\mathrm{n}\}\ n\ i=1 \quad . \quad (5)$$

$$\lfloor\sqrt{2k}\rfloor\leq b1\leq b2\leq \cdots \leq bn\leq\lfloor\sqrt{2k}\rfloor+2. \quad (6)$$

$$Cmin(b1,b2,\ldots,bn) = k/\ n \quad (7)$$

.

$$EMSE(b1,b2,\ldots,bn)=1/n\times 12\sum[bi2-(-2)(bi+1)mod]\ n\ i=1\ . \quad (8)$$

The lower and upper bounds of n are n=1 and n= H×V, the resolutions of a cover image, respectively. The lower and upper bounds of k are k=1 and k=64, respectively, since 264 is the largest integer implemented by the C programming language. Table II shows a number of optimal bases for different parameters of (n, k), where n is in the range of 3 and11, and k is in the range of 4 and 25, which offers the minimal embedding rate $Cmin$ from 1.25 to 2.2727 bpp. An aggressive bit encoding and decomposition scheme (ABED) is proposed, which offers a

TABLE II
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

larger capacity, as shown in the right column, which will be detailed later. C. Aggressive Bit Encoding and Decomposition (ABED) The optimal base provides the maximal pixel change patterns T shown in (4), thus offering the embedding capacity of at least k bits in a pixel group of n pixels. When T is not a power of 2, the difference, h=T-2k, is a positive value, which represents pixel change patterns that still can be exploited. Thus, the embedding capacity offered in a pixel group becomes (k+1) bits, which is larger than the original payload. Inspired by this observation, we present an aggressive bit encoding and decomposition (ABED) scheme. Assume that given (n, k), the optimal base $OB = (b1,b2,\ldots,bn)$ is derived, where themaximal pixel change pattern $T = \prod bi\ n\ i$=1 is available. The ABED scheme first reads k bits of secret message and then determines whether it is possible to convey the next secret bit ($x2$). The ABED scheme consists of three steps, as detailed below.

Step 1: Read in k bits of secret message $S2$ and convert them into the decimal value $S10$. Step 2: Compare $S10$ with the threshold h=T-2k and produce two cases: Case 1: If $S10$<h, it is possible to exploit the residual pixel change patterns. We read in the next secret bit ($x2$) and encode a total of (k+1) bits into the decimal value $S10\ '$, where $S10\ ' = x2 \times 2k + S10$. Case 2: If $S10 \geq$h, we cannot take advantage of the residual pixel change patterns, so simply set $S10\ ' = S10$. Step 3: Decompose $S10\ '$ into n message digits $D(d1,d2,\ldots,dn)$ using (9) by referring to the optimal base $OB = (b1,b2,\ldots,bn)$:

$$di = \{ \quad S10 \mod bi \quad \text{if } i = 1\ \lfloor S10/\prod bj\ i-1\ j=1 \rfloor \mod bi \quad \text{if } 2 \le i \le n. \quad (9)$$

Example 1: an example is presented to illustrate the ABED scheme. Given (n, k)=(3, 4), OB= ($b1$, $b2$, $b3$)=(2, 3, 3), the maximal pixel change pattern is T=2×3×3=18. Let (00011 011011001010…)2 be a serial secret bit stream to be concealed. In step 1,

International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

since k=4, read 4 secret bits $S2$=(0001)2 and convert them into $S10$=1. In step 2, compare $S10$ and the threshold h=18-24=2. Since $S10$<h, case 1 holds. We read in the fifth secret bit $x2$=(1)2, shown with the underlining, and encode 5 secret bits "00011" into the decimal value $S10'$=1×24+1=17. In

TABLE III

GIVEN (N, K)=(3, 4), THE ABED SCHEME FIRST ENCODES 4-5 SECRET BITS AND THEN DECOMPOSES THEIR DECIMAL VALUE S'_{10} INTO 3 MESSAGE DIGITS (d_1, d_2, d_3) USING THE OPTIMAL BASE OB=(2, 3, 3)

S'_{10}	S_2	(d_1, d_2, d_3)	S'_{10}	S_2	d_1, d_2, d_3
0	0000 + 0	0, 0, 0	9	1001	1, 1, 1
1	0001+ 0	1, 0, 0	10	1010	0, 2, 1
2	0010	0, 1, 0	11	1011	1, 2, 1
3	0011	1, 1, 0	12	1100	0, 0, 2
4	0100	0, 2, 0	13	1101	1, 0, 2
5	0101	1, 2, 0	14	1110	0, 1, 2
6	0110	0, 0, 1	15	1111	1, 1, 2
7	0111	1, 0, 1	16	0000 + 1	0, 2, 2
8	1000	0, 1, 1	17	0001 + 1	1, 2, 2

step 3, decompose $S10'$ into 3 message digits $D(d1,d2,d3)$=(1, 2, 2), using (9). In particular, $d1$=17 mod 2=1, $d2$= ⌊17/2⌋ mod 3 = 2, and $d3$=⌊17/(2×3)⌋ mod 3=2.

This example demonstrates that 5 secret bits are concealed. This advances the original embedding capacity of conveying 4 secret bits, even though there are only T=18 maximal pixel change patterns. Note that if the 4 secret bits are (0000)2, it is still possible to convey an extra bit ($x2$). In particular, if $x2$=(0)2, we encode 5 secret bits "00000" into the decimal value $S10'$=0. Alternatively if $x2$ =(1)2, the decimal value being encoded is $S10'$=16. Table III lists detailed decimal values that are encoded and the 3 message digits produced after the decomposition. Note that in this example, the ABED is able to carry an extra bit when the first 4 secret bits are (0000)2 or (0001)2. D. Message Digit Embedding Thus far, k or k+1 secret bits have been concealed and n message digits $D(d1,d2,\ldots,dn)$ have been produced. This section embeds every message digit into every pixel in a pixel group. Since an OpenEXR HDR image has three chromatic channels, the embedding will follow the order of red, green and blue channels. Without loss of generality, take the red channel as an example. Let Pi represent the i-th cover pixel in a pixel group; it has the corresponding sign value (SNi), exponent value (Ei) and mantissa value (Mi). The scenario of embedding the message digit di into Mi involves producing the stego mantissa Mi' such that (Mi' mod bi)= di and the variation ($Mi'-Mi$)2 is minimized. Three steps are required to accomplish the message digit embedding.

Step 1: Compute the current remainder ri using (10). Note that since the mantissa field contains 10 bits, the decimal value of Mi is in the range between 0 and 1023. Step 2: Derive the difference vi using (11). Note that bi is added to ensure that the difference is positive. Step 3: Produce the stego mantissa Mi' using (12). This takes advantage of the modulus operator ensuring to minimize the variation ($Mi'-Mi$)2.

$$ri=Mi \bmod bi. \quad (10)$$

$$vi=[(di-ri)+bi] \bmod bi. \quad (11)$$

$$Mi' = \{Mi \text{ if } vi = 0 \quad Mi+vi \text{ if } 0 < vi < \lfloor bi/2 \rfloor \quad Mi+vi-bi \text{ if } \lfloor bi/2 \rfloor \le vi < bi. \quad (12)$$

Example 2: an example is presented to illustrate the digit message embedding. Given (n, k)=(3, 4), OB=($b1$, $b2$, $b3$)=(2, 3, 3), message digits $D(d1,d2,d3)$=(1, 2, 2) are produced when concealing a secret 5-bit stream (00011)2. Without loss of generality, let ($P1$,$P2$,$P3$)=(0.49902343750, 0.80517578125, 1.01074218750) be three cover pixels in a pixel group, as shown in Table IV. Referring to (1), we derive the decimal value of ($SN1$,$SN2$,$SN3$)= (0, 0, 0), ($E1$,$E2$,$E3$)=(13, 14, 15), and ($M1$,$M2$,$M3$)= (1020, 625, 11), respectively. We employ three steps to conceal ($d1$,$d2$,$d3$)=(1, 2, 2) into ($M1$,$M2$,$M3$)= (1020, 625, 11). In the first step, we compute ($r1$, $r2$, $r3$)=(1020 mod 2, 625 mod 3, 11 mod 3)=(0, 1, 2). Then, we derive the difference ($v1$,$v2$,$v3$)=(1, 1, 0) in the second step. Finally, we produce the stego mantissa ($M1'$,$M2'$,$M3'$)=(1020+1-2, 625+1-3, 11)=(1019, 623, 11). It is possible to derive the floating point value of three stego pixels ($P1'$,$P2'$,$P3'$) = (0.49877929688, 0.80419921875, 1.01074218750). E. Message Extraction The message extraction is performed in the reverse order. Assume that the decoder is given the same embedding parameters (n, k), has been notified that the ABED scheme was employed, and holds the pixel embedding order derived from secret keys. Secret messages can be extracted using the following three steps, as shown in Fig. 3. First, given (n, k), the decoder produces the optimal base OB=($b1$,$b2$,…,bn) and the maximal pixel change patterns T=$\prod bi$ n i=1 . Then, the first pixel group of n pixels is accessed to derive the mantissa value, where n message digits can be extracted using (13),

and the encoded decimal value $S10'$ can be derived by (14). Finally, the concealed binary secret bit $S2'$ is derived using (15). Note that the decimal-to-binary function DB($S10'$,t) converts the decimal value $S10'$ into t bits of binary bit $S2'$. In this equation, the operator "+" conjoins k bits and a single bit $x2$ = (0)2 or (1)2.

TABLE IV
EMBEDDING THREE MESSAGE DIGITS (1, 2, 2) INTO A COVER PIXEL GROUP (P_1, P_2, P_3) TO PRODUCE A STEGO PIXEL GROUP (P'_1, P'_2, P'_3)

Type	Pixel	Floating Value	Sign Deci.	Exponent Deci.	Mantissa Deci.
Cover	P_1	0.49902343750	SN_1 0	E_1 13	M_1 1020
	P_2	0.80517578125	SN_2 0	E_2 14	M_2 625
	P_3	1.01074218750	SN_3 0	E_3 15	M_3 11
Stego	P'_1	0.49877929688	SN_1 0	E_1 13	M'_1 1019
	P'_2	0.80419921875	SN_2 0	E_2 14	M'_2 623
	P'_3	1.01074218750	SN_3 0	E_3 15	M'_3 11

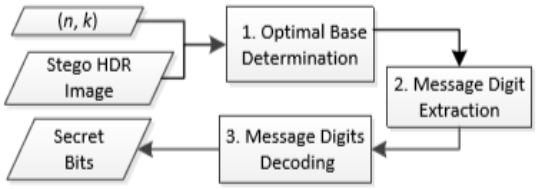


Fig. 3. Flowchart of message extraction in three processes

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

Example 2: an example is presented to illustrate the digit message embedding. Given (n, k)=(3, 4), OB=($b1$, $b2$, $b3$)=(2, 3, 3), message digits $D(d1,d2,d3)$=(1, 2, 2) are produced when concealing a secret 5-bit stream (00011)2. Without loss of generality, let ($P1$,$P2$,$P3$)=(0.49902343750, 0.80517578125, 1.01074218750) be three cover pixels in a pixel group, as shown in Table IV. Referring to (1), we derive the decimal value of ($SN1$,$SN2$,$SN3$)= (0, 0, 0), ($E1$,$E2$,$E3$)=(13, 14, 15), and ($M1$,$M2$,$M3$)= (1020, 625, 11), respectively. We employ three steps to conceal ($d1$,$d2$,$d3$)=(1, 2, 2) into ($M1$,$M2$,$M3$)= (1020, 625, 11). In the first step, we compute ($r1$, $r2$, $r3$)=(1020 mod 2, 625 mod 3, 11 mod 3)=(0, 1, 2). Then, we derive the difference ($v1$,$v2$,$v3$)=(1, 1, 0) in the second step. Finally, we produce the stego mantissa ($M1'$,$M2'$,$M3'$)=(1020+1-2, 625+1-3, 11)=(1019, 623, 11). It is possible to derive the floating point value of three stego pixels ($P1'$,$P2'$,$P3'$) = (0.49877929688, 0.80419921875, 1.01074218750). E. Message Extraction The message extraction is performed in the reverse order. Assume that the decoder is given the same embedding parameters (n, k), has been notified that the ABED scheme was employed, and holds the pixel embedding order derived from secret keys. Secret messages can be extracted using the following three steps, as shown in Fig. 3. First, given (n, k), the decoder produces the optimal base OB=($b1$,$b2$,…,bn) and the maximal pixel change patterns T=$\prod bi\ n\ i$=1 . Then, the first pixel group of n pixels is accessed to derive the mantissa value, where n message digits can be extracted using (13), and the encoded decimal value $S10'$ can be derived by (14). Finally, the concealed binary secret bit $S2'$ is derived using (15). Note that the decimal-to-binary function DB($S10'$,t) converts the decimal value $S10'$ into t bits of binary bit $S2'$. In this equation, the operator "+" conjoins k bits and a single bit $x2$ = (0)2 or (1)2

$$di' = Mi' \bmod bi, \text{i}=1,2,\ldots,\text{n}. \quad (13)$$

$$S10' = d1' + \sum[din'i = 2 \times (\prod bji - 1j = 1)]. \quad (14)$$

$$\text{S2} = \begin{cases} DB(S10',k)+(0)2, & \text{if } 0 \le S10' < T-2k, \\ DB(S10',k) & \text{if } T-2k \le S10' < 2k, \\ DB(S10'-2k,k)+(1)2 & \text{if } S10' \ge 2k. \end{cases} \quad (15).$$

Example 3: an example is presented to illustrate the message extraction. Given (n, k)=(3, 4), OB=($b1$, $b2$, $b3$)=(2, 3, 3), and a stego pixel group ($P1'$,$P2'$,$P3'$)=(0.4987792968750,0.804199218750,1.010742 18750). In the first step, we derive the stego mantissa value ($M1'$,$M2'$,$M3'$)=(1019, 623, 11) and extract three message digits $D(d1',d2',d3')$=(1, 2, 2) using (13). Next, we derive the encoded decimal value $S10'$ = 1+2×2+2× (2×3)=17 using (14). Finally, since $S10' \ge 24$, the third formula shown in (15) is applied to derive secret bits $S2'=DB(17-24,4)+(1)2=(0001)2+(1)2=(00011)2$. Other pixel groups are similarly extracted. F. An Analysis of the ABED Scheme We analyze the expected embedding rate in bit per pixel (bpp) offered by the ABED scheme, which has a close relation to the appearance of the secret bits "0" or "1." Let p represent the appearance probability of secret bit "1." First, we discuss the case for p=0.5. The appearance probability of k bits of "1" is (1/2)k. Referring to the ABED scheme shown in Case 1, when $S10$< (T-2k), it is possible to conceal (k+1) bits, so the expected capacity in this case is C1 =$[(T-2k)/2k]\times$(k+1). Referring to Case 2, when $S10 \ge$T-2k, it is only possible to embed k bits, so the expected payload in this case is C2=$[(2k+1-T)/2k]\times$k. Consequently, the expected embedding rate in bpp offered by the ABED scheme is to sum two terms over n pixels, as shown in (16), where $k = \lfloor \log 2\ T \rfloor$ and $T = \prod bi.\ n\ i$=1

CABED(n,k,T) = C1+C2/ n = 1/ n(k + T−2k /2k). (16)

This equation demonstrates two important features. First, the proposed ABED scheme can conceal an extra rate of (T − 2k)/(n×2k) bpp when the secret bits "0" or "1" have an equal probability of appearance, i.e., p=0.5. Second, the pixel variation caused by concealing this extra payload does not increase because the same optimal base is used. In other words, the ABED scheme provides a significant benefit, increasing payload without augmenting the pixel variation. Some expected capacities using different optimal bases are given in the right column of Table II. Following Example 1, the expected embedding rate CABED(3, 4, 18)=1.375 bpp is higher than the minimal rate Cmin=1.3333 of only using 24 pixel change patterns rather than exploiting a total of T=18 pixel change patterns. If a cover HDR image has the resolution of 3672×3338, the ABED scheme can conceal 510436 additional bits. Statistics show that the range of additional bits concealed is between 83743 and 650806 bits. The general case for the variable p is now discussed, where 0≤p≤1. Take (n, k)=(3, 4) as an example, which has the derived OB=(b1, b2, b3)=(2, 3, 3) and T=2×3×3=18. Table V shows the bit patterns, decimal values (i) and corresponding

TABLE V
THE PROBABILITY FOR DIFFERENT BIT PATTERNS WITH (N, K)-(3, 4)

Pattern	i	P_i	C_i	Pattern	i	P_i	C_i
0000	0	$(1-p)^4$	5	1000	8	$p(1-p)^3$	4
0001	1	$(1-p)^3p$	5	1001	9	$p^2(1-p)^2$	4
0010	2	$(1-p)^3p$	4	1010	10	$p^2(1-p)^2$	4
0011	3	$(1-p)^2p^2$	4	1011	11	$p^3(1-p)$	4
0100	4	$(1-p)^3p$	4	1100	12	$p^2(1-p)^2$	4
0101	5	$(1-p)^2p^2$	4	1101	13	$p^3(1-p)$	4
0110	6	$(1-p)^2p^2$	4	1110	14	$p^3(1-p)$	4
0111	7	$(1-p)p^3$	4	1111	15	p^4	4

appearance probability (Pi) from P0 to P15, where Ci indicates the bits that can be concealed. For example, the bit pattern "0001" equivalent to the decimal i=1 has the corresponding appearance probability P1 =(1-p)3p. The previous discussion indicates that it is possible to conceal 5 secret bits when the bit patterns are "0000" or "0001" equivalent to the decimal value of i=0 and 1. Other bit patterns can only conceal 4 secret bits equivalent to the decimal value of i=2 to 15. Consequently, (17) is a polynomial function derived in the variable p to represent the expected capacity offered by the proposed ABED scheme for the parameters (n, k)=(3, 4), OB=(2, 3, 3) and T=18.

ECABED(p)=13$\sum$(Pi15 i=0 ×Ci) = 13(5−3p+3p2 −p3). (17)

When p=0.5, the expected embedding rate is ECABED(p = 0.5) =1.375 bpp, which is coincident with the value calculated by (16). When p=0.0, ECABED(p = 0.0) has the maximal expected rate (5/3) equivalent to ⌈log2 18⌉/3. However, when p=1.0, ECABED(p = 1.0) has the minimal expected rate (4/3) equivalent to ⌊log2 18⌋/3. The embedding rate in bpp offered by the ABED scheme must be within these two extremes. The polynomial function ECABED(p) reveals that the smaller the p value, the larger the expected capacity, and vice versa. Inspired by this feature, we introduce the bit inversion embedding (BIE) technique. In particular, when a serial secret bit stream to be concealed has the characteristic that the appearance probability of secret bit "1" is greater than 0.5 (p>0.5), we can activate the BIE technique. First, we invert all of the secret bits from "0" to "1" or "1" to "0" before concealing them. This means that all secret bits are conveyed using a new probability p' where p'=1-p, which produces a larger expected capacity ECABED(p'). As an example, assume p=0.65; we activate the BIE scheme for message embedding. Thus, the expected embedding rate produced isECABED(p' = 0.35)=1.424875 bpp, which is greater than ECABED(p = 0.65) =1.347625, increasing by 5.73% of the expected embedding rate.

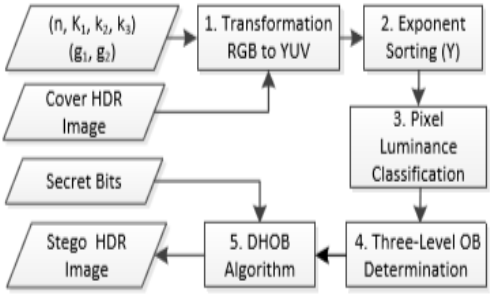


Fig. 4. Flowchart of adaptive message embedding in the proposed ADHOB algorithm

G. An Extension to Adaptive Message Embedding

Our algorithm can be extended to achieve adaptive message embedding, as shown in Fig. 4. The main scenario of adaption is conveying more secret bits in pixels with low luminance, and vice versa. This takes advantage of the human visual sensitivity (HVS) because human beings are less sensitive to the alternation of pixels with low luminance. The embedding parameters of the adaptive algorithm (ADHOB) include (g1, g2), (n,

k1, k2, k3) and a serial secret bit stream (S2). It takes five steps to convey secret messages. Step 1: Transform every pixel Pi represented in the RGB color space to the YUV color space Qi, i=1, 2, …, H×V represented by the IEEE 754 standard single-precision floating-point format, which contains 1-bit sign (sn), 8-bit exponent (e), and 23-bit mantissa (m). Step 2: Sort all of the exponent values (e) in the Y channel from the largest to the smallest and break ties by the scan-line sequential order followed by the pixel position in a scan-line. This produces sorted pixels SQi, i=1, 2, …, H×V. Accordingly, we update the order of pixels in the RGB colors pace to produce sorted pixels (SPi). Step 3: Referring to the parameters (g1, g2), we conduct the pixel luminance classification process

TABLE VI

FEATURES OF 15 TEST HDR IMAGES WITH DIFFERENT DYNAMIC RANGE (DR) IN LOG_{10} AND KEY VALUE (k_y) FOR GROUP-1(LEFT) AND GROUP-2 (RIGHT) IMAGE DATABASES

I	Width	Height	DR	k_y	I	Width	Height	DR	k_y
1	4288	2848	3.88520	0.7090	1	760	1016	3.00818	0.4150
2	2848	4288	6.23260	0.4162	2	760	1016	2.19367	0.4752
3	2845	4275	6.93965	0.3664	3	1024	676	2.33615	0.3423
4	4288	2412	6.96010	0.5991	4	1536	2048	3.40376	0.2171
5	4288	2412	5.28386	0.4558	5	1536	2048	3.03978	0.3062
6	2848	4288	5.33957	0.4919	6	720	480	4.42570	0.3894
7	4288	2412	4.07576	0.4510	7	767	1023	3.73443	0.3711
8	4288	2412	7.59602	0.3725	8	644	874	4.67840	0.4415
9	4288	2412	2.24800	0.5847	9	1024	1024	2.50882	0.6817
10	4288	2412	4.71188	0.5133	10	512	768	3.81602	0.3413
11	4288	2412	4.33039	0.5267	11	720	480	4.12020	0.2979
12	4288	2847	4.33695	0.6220	12	2048	1536	1.88605	0.4190
13	4288	2848	4.25682	0.5562	13	1024	1024	2.50385	0.5010
14	4288	2848	6.07420	0.4763	14	575	575	9.17681	0.8672
15	4288	2848	4.10395	0.5791	15	3720	1396	2.23073	0.6009

classify luminance of the sorted pixels SPi into high, middle and low luminance levels. For simplicity, represent pixels in the high, middle and low level by {L1}, {L2} and {L3}, respectively. {L1} contains g1 percentage of pixels, {L2} has (g2-g1) percentage of pixels, and {L3} consists of (100-g2) percentage of pixels. Step 4: Determine three optimal bases, $OH1$,$OH2$ and $OH3$ corresponding to {L1}, {L2} and {L3} according to the embedding parameters (n, k1), (n, k2) and (n, k3). Step 5: Referring to the secret bit stream (S2), embed k1, k2 and k3 bits into every pixel group at {L1}, {L2} and {L3} using the proposed data hiding algorithm. This produces the stego OpenEXR HDR image.

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

IV. EXPERIMENTAL RESULTS AND COMPARISONS

We implemented our scheme in C++ programming language and conducted the experiments in a platform with the Linux operating system. We present the experimental results and compare our algorithm with the state-of-the-art algorithms in the literature.

A. Embedding Capacity Results

Experiments were conducted using two image database (group-1 and group-2), each of which contains 15 images selected from NCHU HDR-EXR database which contains 95 HDR OpenEXR images. Detailed information on the image database is given in the supplemental material A. We remark that while most of them were downloaded from the Internet available to the public [7] [31] [32], seven HDR images in the group-2 image database are derived from real scenes corresponding to the actual measured luminance. The binary contents of the Open EXR image, 507, represent a serial secret bit stream to be concealed.

Table VI show fundamental features of the test images in two image databases, indexed from 1 to 15. In addition, minimal and maximal pixel values and the pixel patterns used in our experiments are shown in supplemental material B. Reinhard et al. [18] first classified HDR images α based on the logarithmic average luminance with respect to the minimal and maximal luminance values [22] [29] [30]. Later, Akyuz and Reinhard adopted the normalized log-average luminance of an HDR image to approximate the key value (ky) of the scene [31] [32]. Both α and ky indicate whether a scene is subjectively light, normal, or dark. In our experiments, we selected images with a variety of ky values.

TABLE VII

THE CAPACITY OFFERED BY OUR DHOB ALGORITHM IN GROUP-1 (TOP) AND GROUP-2 (BOTTOM) IMAGE DATABASES

I	k	ABED	ABED-BIE	VSI	PPCC	SRCC	T(s.)
1	3	38139960	38259650	0.999979	0.999925	0.999924	354.9
3	5	62312076	62429606	0.999994	0.999944	0.999921	371.1
5	8	84244089	84378136	0.999974	0.999819	0.999843	343.9
7	11	114508458	114600559	0.999918	0.999812	0.999818	357.5
9	14	145091872	145148460	0.999591	0.999741	0.999824	376.3
11	17	175942133	175970287	0.999730	0.999735	0.999340	402.1
13	19	232043664	232045620	0.997450	0.999640	0.998512	479.2
15	21	256456683	256456683	0.985669	0.999630	0.997441	502.4
I	k	ABED	ABED-BIE	VSI	PPCC	SRCC	T(s.)
2	3	2413825	2418571	0.999384	0.999940	0.999927	59.0
4	5	16118549	16146177	0.999884	0.999925	0.999917	149.0
6	7	2478707	2481168	0.986751	0.999822	0.999827	46.3
8	9	5065686	5065686	0.999930	0.999806	0.999715	54.1
10	11	4353995	4356410	0.998529	0.999833	0.999625	49.0
12	13	40969947	40984182	0.999956	0.999814	0.999111	164.2
14	15	4959360	4959360	0.999306	0.999710	0.998791	48.2
15	16	83094288	83094568	0.998589	0.999622	0.997423	245.1

THE CAPACITY OFFERED BY OUR ADHOB ALGORITHM IN GROUP-1 (TOP) AND GROUP-2 (BOTTOM) IMAGE DATABASES

I	k_1-k_3	ABED	ABED-BIE	VSI	PPCC	SRCC	T(s.)
2	3-5	46126523	46247629	0.999998	0.998502	0.997431	413.3
4	5-7	59923890	60002560	0.999986	0.998032	0.997622	365.7
6	7-10	98356111	98499490	0.999909	0.999003	0.997523	438.3
8	10-13	111578813	111659564	0.999983	0.999419	0.999228	396.9
10	13-18	172389162	172396604	0.999849	0.999310	0.999715	443.0
12	18-20	228396201	228397476	0.996168	0.999216	0.999022	518.0
14	22-24	276828421	276831140	0.990024	0.998733	0.998328	554.3
15	23-25	288042932	288046640	0.972725	0.997015	0.997418	558.7
I	k_1-k_3	ABED	ABED-BIE	VSI	PPCC	SRCC	T(s.)
1	2-4	2148813	2151079	0.999960	0.999813	0.999844	72.56
3	4-6	3261169	3266863	0.999968	0.999720	0.999113	65.92
5	6-8	21036596	21051014	0.999861	0.999922	0.998004	170.97
7	8-10	6918525	6922941	0.999760	0.999316	0.999624	72.68
9	10-12	11295899	11303030	0.999741	0.999022	0.999113	83.45
11	12-14	4363473	4363865	0.988710	0.999095	0.999192	53.27
13	14-16	15427919	15430391	0.989069	0.998611	0.998330	82.24
15	16-18	86564731	86569609	0.998790	0.997002	0.997405	328.57

The embedding capacities for group-1 and group-2 image databases are shown in the first four columns of Table VIII. Detailed statistics for k=3 to 21 are shown in supplemental material C. We remark that HDR test images in group-1 have a larger resolution, thus offering higher embedding capacity when using the same embedding parameter. When adopting bit inversion embedding (BIE) in both algorithms by flipping the bits first before embedding, we obtain a larger embedding capacity. Using k=7 in group-1, for example, 122569 extra bits can be concealed, producing an embedding rate of 7.1808 bits per pixel. Our experiment shows that the average appearance of the probability for bit "1" in the contents of the HDR "507" image is p=0.5056076. Since p>0.5, it is beneficial to activate the BIE scheme to increase the embedding capacity. It is interesting to note that when k= 9, 12, 15, 18, or 21, the maximal pixel change patterns (T) derived from the optimal base is a power of 2. It is not possible to encode an extra bit, nor is the capacity influenced by the probability p. Consequently, the capacity does not change when activating the BIE. The embedding capacities using ADHOB algorithm are shown in the first four columns of Table VIII. The threshold (g1, g2)=(25%, 60%) is set, which means that 25% of pixels are classified into the high luminance level, another 35% of pixels are classified into the middle luminance level and the remaining pixels are in the low luminance level. At each level, (k1, k2, k3)

bits are concealed in a pixel group of 3 pixels (n=3). These statistics confirm that the BIE scheme does offer an advantage in providing greater embedding capacities.

TABLEVIII

B. Image Quality Results

While the inverse tone mapping converts low dynamic range (LDR) images to HDR ones [33], tone mapping addresses the problem of strong contrast reduction from scene radiance to the displayable ranges while preserving the image details and color appearance [34]. We adopt an open source package, Luminance HDR [35], as our HDR test software. Formerly Qtpfsgui, this graphics software supports several graphic formats, including OpenEXR and Radiance RGBE. Various tone mapping operators (TMOs) are implemented including Mantiuk06 and Mantiuk08. Users can exchange experience and information through community websites such as Flickr and Facebook. The next three columns of Table VII show the image quality results for group-1 and group-2 image databases using DHOB algorithm.We display visual saliency-based index (VSI) between the cover and stego tone-mapped images [36] [37] using the default settings, which is perceptual image quality assessment aiming to use computational models to measure the image quality. The VSI values are close to 1.0 showing that the stego images are similar to the cover image with a high perceptual image quality. The image quality measured from the structural similarity index (SSIM) [38] and information content weighted SSIM index (IW-SSIM) [39] produces similar results, which are detailed in the supplemental material C. Pearson's product-moment correlation coefficient (PPCC) [40] and Spearman's rank correlation coefficient (SRCC) [41] between the histogram of tone-mapped cover and stego images are close to 1.0, showing a strong linear dependency between cover and stego images. Finally, shown in the last column, the execution time

required to embed secret messages is less than 502.4 seconds. Our experiment indicates that nine-tenth of the time is spent in Input/Out, including reading and storing an HDR image and constructing dynamic data structures to process the mantissa field for message embedding and extraction

TABLE IX
PIXEL RATIOS (R%) UNDER DIFFERENT DETECTION PROBABILITY (P) USING DHOB ALGORITHM FOR STEGO LDR IMAGES (TOP) AND STEGO HDR IMAGES (BOTTOM) IN THE GROUP-1 IMAGE DATABASE

I	k	p≤0.25	.25-.5	.5-.75	.75-.95	p>.95	Q (L)
2	4	100.00	0.00	0.00	0.00	0.00	99.93
4	7	100.00	0.00	0.00	0.00	0.00	99.84
6	10	100.00	0.00	0.00	0.00	0.00	96.73
8	13	100.00	0.00	0.00	0.00	0.00	92.26
10	16	97.75	1.72	0.45	0.08	0.00	75.07
12	18	78.68	7.84	5.46	4.78	3.23	69.38
14	20	90.14	4.81	2.45	1.43	1.17	63.01
I	k	p≤0.25	.25-.5	.5-.75	.75-.95	p>.95	Q (H)
2	4	100.00	0.00	0.00	0.00	0.00	99.99
4	7	100.00	0.00	0.00	0.00	0.00	100.00
6	10	100.00	0.00	0.00	0.00	0.00	99.83
8	13	100.00	0.00	0.00	0.00	0.00	93.91
10	16	100.00	0.00	0.00	0.00	0.00	85.54
12	18	100.00	0.00	0.00	0.00	0.00	79.33
14	20	100.00	0.00	0.00	0.00	0.00	83.52

image quality results for group-1 and group-2 image databases using ADHOB algorithm are shown in the next three columns of Table IX. The VSI, PPCC and SRCC values are displayed, while SSIM and IW-SSIM statistics are shown in the supplemental material C. All statistics are close to 1.0 which demonstrates a high similarity between cover and stego images. This is due to the fact that secret messages are concealed in the mantissa field with 10 bits of length, thus producing a small distortion. Finally, while the execution time is less than 558.7 seconds, the time required to process images in group-2 is faster since they have smaller resolutions. In general, adaptive message embedidng requires longer time because more steps are needed to conceal messages.

C. The HDR-VDP-2 Results

An HDR visual difference predictor [42] [43] [44] compares a pair of host and test images. We adopted the HDR-VDP-2 (version 2.2.1) which is a major revision of the original HDR-VDP to improve the accuracy of the predictions. This metric is based on a calibrated visual model that can reliably predict visibility and quality differences between image pairs. A two-dimensional map with the probability of detection at each pixel point is produced to exhibit the likelihood that an average observer would notice a difference between cover and stego images. We show the statistics of both tone-mapped stego LDR image and stego HDR image. Detailed statistics for k=3 to 21 are shown in the supplemental material D. Since HDR-VDP-2 does not provide an option to automatically output the ratio of pixels, we collected these statistics based on the probability of the detection map. We presented the LDR image quality values, Q(L), which shows the visual quality of the tone-mapped stego images. An HDR image quality value, Q(H), which reveals the visual quality of an HDR stego image was also given. The higher the image quality value (up to 100),

TABLE X
PIXEL RATIOS (R%) UNDER DIFFERENT DETECTION PROBABILITY (P) USING ADHOB ALGORITHM FOR STEGO LDR IMAGES (TOP) AND STEGO HDR IMAGES (BOTTOM) IN THE GROUP-2 IMAGE DATABASE

I	k_1-k_3	p≤0.25	.25-.5	.5-.75	.75-.95	p>.95	Q (L)
1	(2, 3, 4)	100.00	0.00	0.00	0.00	0.00	99.42
3	(4, 5, 6)	100.00	0.00	0.00	0.00	0.00	99.13
5	(6, 7, 8)	100.00	0.00	0.00	0.00	0.00	99.68
7	(8,9,10)	100.00	0.00	0.00	0.00	0.00	97.77
9	(10,11,12)	100.00	0.00	0.00	0.00	0.00	90.93
11	(12,13,14)	99.07	0.53	0.17	0.09	0.14	83.63
13	(14,15,16)	91.66	3.51	1.65	1.02	2.16	79.12
I	k_1-k_3	p≤0.25	.25-.5	.5-.75	.75-.95	p>.95	Q (H)
1	(2, 3, 4)	100.00	0.00	0.00	0.00	0.00	99.96
3	(4, 5, 6)	100.00	0.00	0.00	0.00	0.00	99.98
5	(6, 7, 8)	100.00	0.00	0.00	0.00	0.00	99.92
7	(8,10,11)	100.00	0.00	0.00	0.00	0.00	96.85
9	(11, 13,16)	100.00	0.00	0.00	0.00	0.00	99.20
11	(17,18,19)	100.00	0.00	0.00	0.00	0.00	98.54
13	(14,15,16)	100.00	0.00	0.00	0.00	0.00	98.72

the greater the perceptual similarity between the cover and stego images. The tone-mapped statistics show that when k≤20, r≥97.4% for p≤0.5 and Q(L) is over 63.01. When k=18-20, r≤8.01% for p≥0.75. In addition, the HDR statistics show that when k≤20, r=100.0% for p≤0.25 and Q(L) is over 79.33. This indicates a significantly low probability that the differences between the cover and stego images are visible to an average observer. We suggest that the largest parameter setting for k is no greater than 20 for the DHOB algorithm.

D. The tone-mapped statistics

show that when the embedding parameters ($k1$,$k2$,$k3$)=(14, 15, 16), r≥95.17% for p≤0.5 and r≤3.18% for p>0.75. The Q(L) is over 79.12. In addition, the HDR statistics show that when k≤16, r=100.0% for p≤0.25 and the Q(H) are over 96.85. Statistics show a small ratio of pixels for a high probability of detection, which means that the differences between the cover and stego images are not visible to an average viewer. Fig. 5 presents the probability of detection maps reported by the HDR-VDP-2 using tone-mapped stego LDR (VDPL) and

stego HDR images (VDPH) for the group-1 image database. Images with a larger resolution are shown in the supplemental materials D and E. Most maps show all blue, indicating a low detection probability of visual difference between the cover and stego images. The tone-mapping operator shrinks the luminance to the displayable range resulting; thus, the VDPL is more senstive than VDPH in revealing the visual difference between the cover and stego images

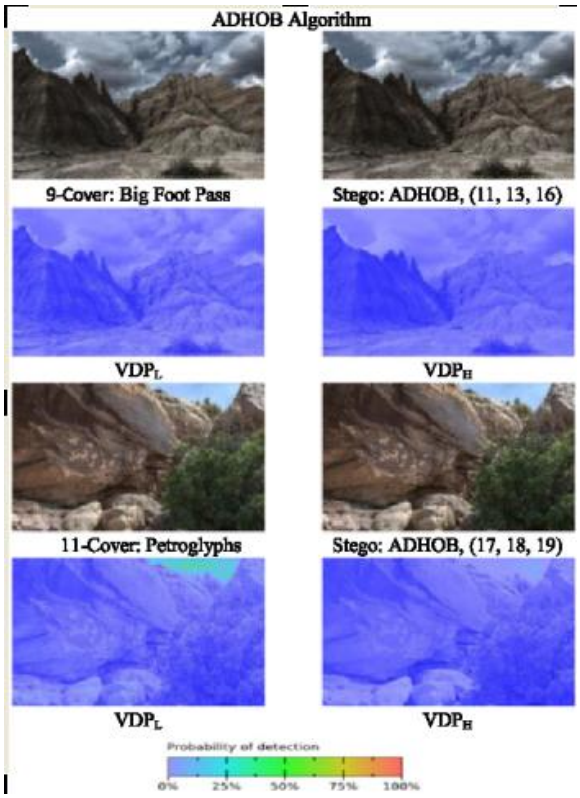


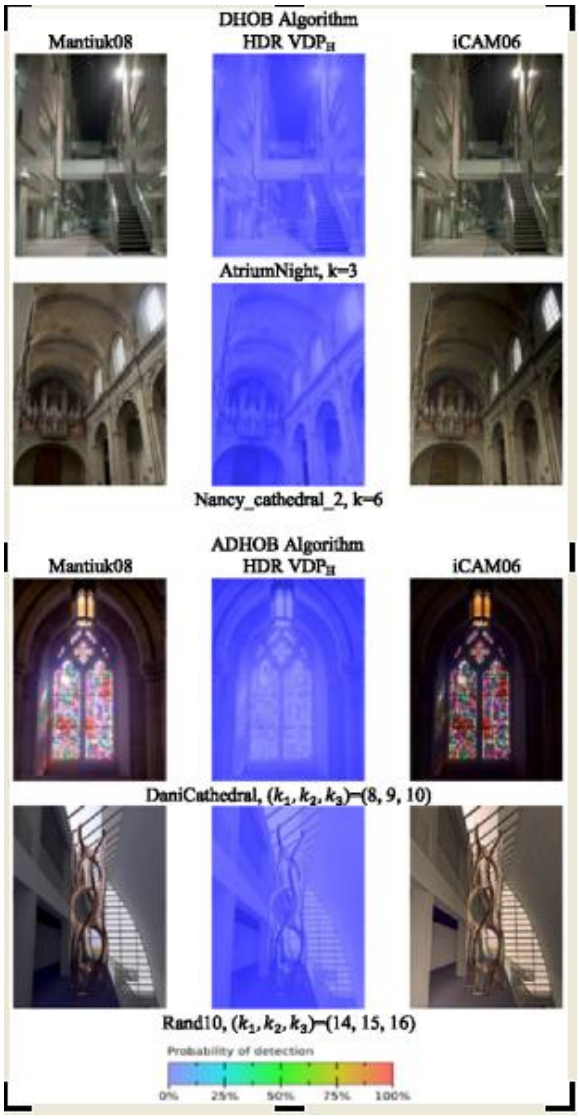
Fig. 5. Results produced by HDR-VDP-2 using both tone-mapped stego LDR (VDPL) and stego HDR images (VDPH) in group-1 image database

colors seem to be more faithful when employing the TMO iCAM06.

. The experimental results are shown in Table XI,

G. The embedding capacity,

ranging from 1.04 to 21.65 million bits, is smaller due to the limited 8-bit storage space in the RGBE format. . All of the statistics of VSI, PPCC and SRCC are close to 1.0, showing a strong linear dependency between cover and stego images. Finally, the execution time is between 2.1 and 32.9 seconds which are mainly affected by the resolutions of the test images. Our experiment shows that the conversion between 48-bit OpenEXR and 32-bit RGBE formats produces a significant change in pixel value. Detailed statistics are presented in the supplemental material H. Under this circumstance,



The experimental results are shown in Table XI,

TABLE XI

CONCEALING SECRET MESSAGES INTO THE RADIANCE RGBE HDR IMAGES USING OUR DHOB ALGORITHM (N=3, K=2-5)

Index	k	ABED-BIE	VSI	PPCC	SRCC	T(s.)
1	2	1544320	0.999995	0.99695	0.99684	3.6
2	3	2447689	0.999992	0.99790	0.99807	5.1
3	4	2886522	0.999993	0.99752	0.99643	4.8
4	5	16263178	0.999996	0.99640	0.99629	22.2
5	2	6291456	0.999996	0.99591	0.99693	26.4
6	3	1095526	0.999961	0.99515	0.99431	2.3
7	4	3271894	0.999985	0.99701	0.99195	5.3
8	5	2909923	0.999880	0.99989	0.99804	3.8
9	2	2097152	0.999778	0.93694	0.95275	5.2
10	3	1246465	0.999943	0.99595	0.99295	2.6
11	4	1441126	0.999966	0.99931	0.99328	2.3
12	5	16263178	0.999997	0.99786	0.98265	20.8
13	2	2097152	0.999974	0.97299	0.99007	5.4
14	3	1048056	0.999974	0.99619	0.99285	2.1
15	4	21654922	0.999992	0.97552	0.96953	32.9

D. The LDR and HDR Steganalysis Results

We present the results of the steganalysis which aim to detect any messages conveyed in an HDR OpenEXR image. We remark that since the stego HDR images generated by our algorithms comply 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. Thus, we adopted the RS steganalysis [26] using tone-mapped LDR stego images to evaluate the detectability of our algorithms. The experimental results of the LDR RS steganalysis in three channels are shown in the top part of Table XIII. In the detection processing, the absolute difference of a regular group (DIR) and that of a singular group (DIS) are computed in the using the recommended default parameters. The proposed algorithms reveal a small absolute difference in both DIR and DIS, indicating that the tone-mapped stego LDR image produced is secure against the LDR RS steganalytic attack. To the best of the authors' knowledge, there are no steganalytic algorithms directly available to detect the existence of concealed messages for high dynamic range images. Nevertheless, we conducted the HDR RS steganalytic attack by directly detecting the mantissa field of HDR stego images since it is the place where we concealed secret messages. In particular, the maximal optimal base we adopted is (323, 323, 323) for k=25. This means that the maximal magnitude of distortion in the 10-bit mantissa field is less than ⌊323/2⌋. Such a distortion does not affect the two most significant bits in the mantissa field. Therefore, we extracted eight least significant bits in the mantissa field in an HDR stego image and constructed a stego HDR-RGB mantissa image, on which we were able to conduct HDR steganalytic attacks to detect any hidden messages within a stego HDR image. The bottom part of Table XII 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 demonstrate that the stego HDR images produced by our algorithms are also secure against the HDR RS steganalyzer. We conducted steganalysis of our algorithm under the LDR SPAM steganalyzer [27] using the tone-mapped stego LDR images. First, we trained the SPAM steganalyzer on the NCHU HDR-EXR database, where we employed the LIBSVM integrated software [45] for training. We adopted the range of differences T=4 and T=3 for the first- and second-order of the Markov chain; thus, in the training process, the first- and second–order features have dimensions 162 and 686, respectively.

TABLE XII

LDR RS (TOP) AND HDR RS (BOTTOM) STEGANALYTIC RESULTS FOR THE "GENERAL GRANT" IMAGE USING DHOB (K=17) AND ADHOB ALGORITHMS (K_1=17, K_2=18, K_3=19)

Type	Channel	R_M (%)	R_{-M} (%)	DIR (%)	S_M (%)	S_{-M} (%)	DIS (%)
LDR Cover	Red	37.80	38.77	0.97	13.42	13.22	0.20
	Green	36.20	36.28	0.08	14.16	14.13	0.03
	Blue	36.68	36.73	0.05	14.75	14.80	0.05
DHOB	Red	36.04	38.07	2.03	18.91	17.82	1.09
	Green	35.04	35.17	0.13	21.30	21.24	0.06
	Blue	35.85	35.95	0.10	19.65	19.62	0.03
ADHOB	Red	35.84	37.95	2.11	20.34	19.17	1.17
	Green	34.82	34.96	0.14	22.88	22.81	0.07
	Blue	35.71	35.78	0.07	20.43	20.43	0.00
HDR Cover	Red	35.11	35.93	0.82	34.96	34.16	0.80
	Green	35.30	35.66	0.36	34.22	33.88	0.34
	Blue	35.97	36.43	0.46	33.68	33.22	0.47
DHOB	Red	35.24	35.73	0.49	34.87	34.40	0.48
	Green	35.09	35.55	0.47	34.45	34.00	0.45
	Blue	35.43	35.84	0.41	34.08	33.65	0.43
ADHOB	Red	35.16	35.77	0.61	34.90	34.30	0.61
	Green	35.08	35.61	0.53	34.47	33.96	0.52
	Blue	35.47	35.86	0.39	34.03	33.63	0.41

Once the training was completed, we evaluated the SPAM steganalyzer performance on the testing set by computing the error rate (PErr) under different parameters; k for DHOB algorithm and (k1, k2, k3) for ADHOB algorithms, which conceal various quantities of secret messages. The error rate is derived by PErr = (PFp+PFn)/2, where PF and PFn stand for the probability of false positive (detection cover as stego) and probability of false negative (missed detection). We conducted the training and evaluation process five times and reported the average error rates. We remark that the higher the average error rates, the lower the detectability. Note

that the SPAM performs the steganalysis of the grayscale images. Thus, we conducted the steganalysis on tone-mapped stego images in three individual channels using the kernel parameters $\gamma 1 = 1/162$, $\gamma 2 = 1/686$, and the cross-validation cv = 5. The top part of Table XIII shows the LDR SPAM steganalytic results using the DHOB algorithm, where the training model is images in our database concealed with secret messages using the embedding parameter k=20. The SPAM steganalyzer shows a high average error rate for the target stego images in the range of PErr=[0.425, 0.588] for the first-order and PErr=[0.425, 0.563] for the second-order, respectively. The average error rates for the second-order are smaller than those of the first-order, indicating that the second-order SPAM features provide greater accuracy of the steganalysis. Nevertheless, both orders show high average error rates representing that our DHOB algorithm is not detectable, despite having dimensions as high as 686 features. The bottom of Table XIII shows the LDR SPAM steganalytic results for the ADHOB algorithm, where we adopted images with the embedding parameter $(k1,k2,k3)=(18, 19, 20)$ as our training model. For the target stego images, the

TABLE XIII
THE AVERAGE ERROR RATES IN PERCENTAGE COLLECTED FROM THE LDR SPAM STEGANALYZER USING THE DHOB (TOP) AND ADHOB ALGORITHMS (BOTTOM) FOR THE GROUP-1 IMAGE DATABASE

Channel	k	3	5	8	11	14	17	19
Red	1st	.588	.563	.575	.525	.525	.463	.475
	2nd	.525	.513	.563	.475	.475	.425	.450
Green	1st	.538	.525	.538	.488	.488	.450	.425
	2nd	.538	.513	.538	.475	.475	.438	.425
Blue	1st	.550	.563	.525	.538	.538	.450	.438
	2nd	.525	.488	.488	.463	.463	.463	.425
	k_1	3	5	7	10	11	16	17
Channel	k_2	4	6	8	11	13	17	18
	k_3	5	7	10	13	16	18	19
Red	1st	.563	.550	.538	.500	.500	.450	.463
	2nd	.538	.513	.513	.488	.488	.425	.450
Green	1st	.550	.538	.550	.488	.488	.450	.488
	2nd	.525	.500	.525	.500	.500	.438	.475
Blue	1st	.563	.563	.550	.525	.525	.425	.463
	2nd	.538	.500	.513	.475	.475	.438	.438

average error rate is in the range of PErr=[0.425, 0.563] for the first-order and in the range of PErr=[0.425, 0.538] for the second-order. These high average error rates led to the low accuracy of the steganalysis. Consequently, the stego images generated by our ADHOB algorithms are also undetectable by the SPAM steganalyzer. Similarly, we performed HDR SPAM steganalysis tests where the training models were constructed by extracting eight least significant bits in the mantissa field from an OpenEXR HDR image with k=16

TABLE XIV
THE AVERAGE ERROR RATES IN PERCENTAGE COLLECTED FROM THE HDR SPAM STEGANALYZER USING THE DHOB (TOP) AND ADHOB ALGORITHMS (BOTTOM) FOR THE GROUP-2 IMAGE DATABASE

Channel	k	2	4	6	9	12	14	16
Red	1st	.501	.491	.512	.524	.528	.507	.468
	2nd	.490	.519	.493	.531	.539	.510	.532
Green	1st	.490	.505	.525	.514	.536	.527	.501
	2nd	.507	.492	.524	.461	.501	.560	.520
Blue	1st	.500	.509	.507	.465	.521	.459	.442
	2nd	.500	.514	.512	.533	.483	.446	.568
	k_1	2	3	6	7	10	11	14
Channel	k_2	3	4	7	8	11	12	15
	k_3	4	5	8	9	12	13	16
Red	1st	.491	.494	.501	.512	.455	.496	.564
	2nd	.508	.496	.486	.509	.499	.480	.559
Green	1st	.497	.482	.502	.511	.497	.523	.444
	2nd	.511	.506	.508	.473	.454	.487	.439
Blue	1st	.486	.508	.496	.525	.452	.520	.496
	2nd	.519	.480	.478	.466	.536	.485	.458

The top part of Table XV shows the HDR SAPAM steganalytic results with the penalization parameters (C1, C2)=(190000, 10100) using the DHOB algorithm. A high average error rate is reported for the target stego HDR images in the range of PErr=[0.442, 0.536] for the first-order and PErr=[0.446, 0.568] for the second-order, respectively. Both orders show a high average error rate around 0.5, which represents that the SPAM steganalyzer is unable to detect stego HDR images produced by the DHOB algorithm. We further performed HDR SPAM steganalysis tests for the ADHOB algorithm using the embedding parameters $(k1, k2, k3)=(15, 16, 17)$. The bottom part of Table XIV shows the results where a high average error rate is reported for the target stego HDR images in the range of PErr=[0.444, 0.564] for the first-order and PErr=[0.439, 0.559] for the second-order, respectively. Both orders show a high average error rate around 0.5, which represents that the HDR 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.

Since the magnitude of the embedding rate in bpp is affected by the maximal space originated from different HDR formats, we instead compared the concealed field ratio (CFR) to provide a fair comparison. The CFR, which is independent of the HDR format, represents the ratio of the bpp over the maximal space (bpp/maximal space). Thus, CFR denotes the percentages of a unit of a one-bit space that can be exploited. Our proposed schemes offer

the highest CFR, being in the range 8.11% and 66.67%, while Wang and Cheng's method provides the smallest range of CFR. 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.

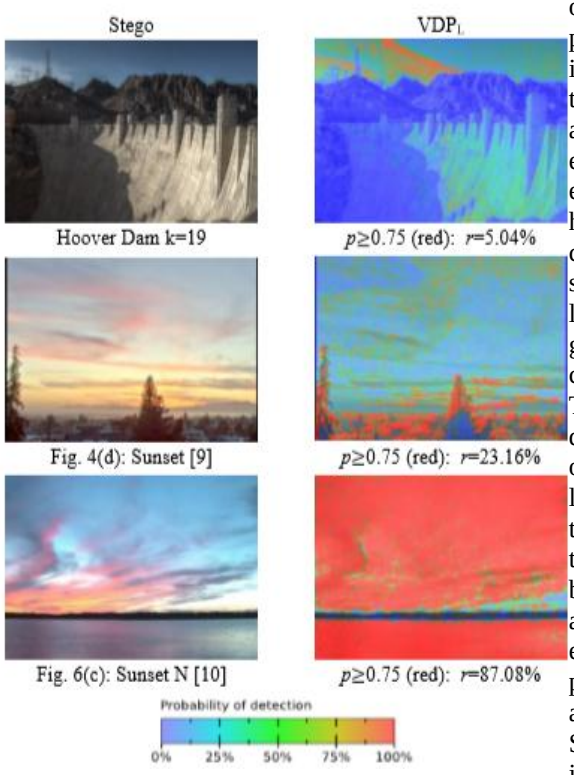


Fig.7. The VDP-2 comparison for results produced by our algorithm, Wang and Cheng's, and Li et al.'s works

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.

V. 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 proposed algorithm is extended to support luminance-aware adaptive data hiding, where the luminance of an HDR image is classified into high, middle and low levels. More secret bits are conveyed in pixels with a low luminance level and vice versa. We adopted two groups of image databases for testing, each of which contains 15 HDR images with different luminance. The results of the HDR visual difference predictor demonstrate that the tone-mapped stego LDR images or stego HDR images have high image quality with a low probability of detection that differences between the cover and stego images are difficult to be visible to an average viewer. A stego HDR image generated by our algorithm preserves the original file format and is unlikely to arouse suspicion from eavesdroppers. 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. The comparison shows that our algorithm has the best results, outperforming the current state-of-the-art schemes. The proposed scheme provides advantages for data hiding

applications such as image annotation and covert communications. While our algorithm already performs well, some further improvements are still possible. Future study will investigate a more effective message encoding method to further increase the embedding capacity.

APPEDIX 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

$$EMSE(b) = \frac{\{02+12+\cdots+(b2)2+[-(b\,2-1)]\,2+\cdots+(-1)2\}}{b} = \frac{b2+2}{12} \quad \text{(A-1)}$$

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.

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

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

2. 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.

3. 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] V. Solachidis, E. Maiorana, P. Campisi, and F. Banterle, "HDR image watermarking based on bracketing decomposition," in Proc. DSP, 2013, Santorini, Greece, pp. 1–6

[14] F. Autrusseau and D. Goudia, "Nonlinear hybrid watermarking for high dynamic range images," in Proc. ICIP, 2013, Melbourne, Australia, pp. 4527–4531.

[15] J. L. Wu, "Robust watermarking framework for high dynamic range images against tone-mapping attacks," Watermarking, vol. 2, InTech: USA, pp. 229–242, 2012.

[16] E. Maiorana, V. Solachidis, and P. Campisi, "Robust multibit watermarking for HDR images in the Radon-DCT domain," in Proc. ISPA, 2013, Trieste, Italy, pp. 284-289.

[17] F Guerrini, M Okuda, N Adami, and R Leonardi, "High dynamic range image watermarking robust against tone-mapping operators," IEEE Trans. Inf. Forensics Sec., vol. 6, no. 2, pp. 283–295, 2011.

[18] X. Xue, T. Jinno, X. Jin, M. Okudada, and S. Goto, "Watermarking for HDR image robust to tone mapping," IEICE Trans. Fundam. of Electron., Commun. Comput. Sci., vol. 94, no. 11, pp. 2334–2341, 2011

[19] T. Bioanchi and A. Piva, "Secure watermarking for multimedia content protection: a review of its benefits and open issues," IEEE Signal Process. Mag., vol. 30, iss. 2, pp. 87-96, 2013.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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).

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] E. Reinhard, M. Stark, P. Shirley, and J. Ferwerda, "Photographic tone reproduction for digital images," ACM Trans. Graph., vol. 21, no. 3, pp. 267–276, 2002.

[30] E. Reinhard, "Parameter estimation for photographic tone reproduction," J. of Graphics Tools, vol. 7, no. 1, pp. 45-52, Nov. 2002.

[31] A. O. Akyuz and E. Reinhard, "Color appearance in high-dynamic-range imaging," J. of Electronic Imaging, vol. 13(3), pp. 1–12, Jul.-Sept. 2006.

[32] P. Hanhart, M. V. Bernardo, M. Pereira, A. M. G. Pinheiro, and T. Ebrahimi, "Benchmarking of objective quality metrics for HDR image quality assessment," EURASIP Journal on Image and Video Processing, vol. 39, pp. 1–18, 2015.

[33] T. H. Wang, C. W. Chiu, W. C. Wu, J. W. Wang, C. Y. Lin, C. T. Chiu, 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.

[34] G. Eilertsen, R. K. Mantiuk, and J. Unger, "Real-time noise-ware tone mapping," ACM Trans. Graph., (Proceedings of SIGGRAPH Asia 2015), vol. 34, iss. 6, article no. 198, Nov. 2015.

[35] Luminance HDR open source. [Online]. Available http://qtpfsgui.sourceforge.net/?page_id=2

[36] L. Zhang, Y. Shen, and H. Li, "VSI: a visual saliency-induced index for perceptual image quality assessment," IEEE Trans. Image Process., vol. 23, no. 10, pp. 4270–4281, Oct. 2014.

[37] The VSI for perceptual image quality assessment. [Online]. Available, http://sse.tongji.edu.cn/linzhang/IQA/VSI/VSI.htm

[38] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.

[39] Z. Wang and Q. Li, "Information content weighting for perceptual image quality assessment," IEEE Trans. Image Process., vol. 20, no. 5, pp. 1185–1198, May 2011.

[40] L. Rodgers and W. A. Nicewander, "Thirteen ways to look at the correlation coefficient," The American Statistician, vol. 42, pp. 59–66, 1988.

[41] G. U. Yule, An Introduction to the theory of statistics (1919), Kessinger Publishing, LLC, Whitefish, MT, USA, Sept. 2010.

[42] R. Mantiuk, K. Myszkowski, and H. P. Seidel, "Visible difference predictor for high dynamic range images," in Proc. of IEEE Int. Conf.

on Syst., Man, Cybern., vol. 3, pp. 2763–2769, 10-13 Oct. 2004.

[43] R. Mantiuk, K. J. Kim, A. G. Rempel, and W. Heidrich, "HDR-VDP-2: A calibrated visual metric for visibility and quality predictions in all luminance conditions," ACM Trans. Graph., vol. 30, no. 4, article No. 40, 2011.

[44] M. Narwaria, R. K. Mantiuk, M. P. Da Silva, and P. Le Callet, "HDR-VDP-2.2: A calibrated method for objective quality prediction of high-dynamic range and standard images," J. of Electronic Imaging, vol. 24, no. 1, 010501, Jan. 2015.

[45] C. C. Chang and C. J. Lin, "LIBSVM: a library for support vector machines," ACM Trans. Intelligent Systems and Tech., vol. 2, no. 3, article 27, pp. 1–27, 2011.