electronics

MDPI

Article

Optimal Weighted Modulus: A Secure and Large-Capacity Data-Hiding Algorithm for High Dynamic Range Images

Ku-Sung Hsieh and Chung-Ming Wang *

Department of Computer Science and Engineering, National Chung Hsing University, Taichung 402202, Taiwan; oudoollo@gmail.com

* Correspondence: cmwang@cs.nchu.edu.tw

Abstract: This paper presents an optimal weighted modulus (OWM) algorithm able to conceal secret messages in a high dynamic range image encoded via the RGBE format, consisting of the red, green, blue, and exponent channels. In contrast to current state-of-the-art schemes, which mainly employ limited and vulnerable homogeneous representations, our OWM scheme exploits four channels and an embedding weight to conceal secret messages, thereby offering more embedding capacities and undetectability against steganalytic tools. To reduce the impact on the luminance variation, we confine the maximal change incurred in the exponent channel when embedding secret messages. In addition, we propose an SEC scheme to eliminate the pixel saturation problem, even though a pixel contains values close to the boundary extreme. As a result, the stego images produced not only exhibit high quality but also comply with the RGBE encoding format, making them able to resist malicious steganalytic detection. The experimental results show that our scheme offers larger embedding rates, between 2.8074 and 5.7549 bits per pixel, and the average PSNR value for twelve tone-mapped images is over 48 dB. In addition, the HDR VDP 3.0 metric demonstrates the high fidelity of stego HDR images, where the average Q value is close to the upper bound of 10.0. Our scheme can defeat RS steganalytic attacks and resist image compatibility attacks. A comparison result confirms that our scheme outperforms six current state-of-the-art schemes.

Keywords: optimal weighted modulus; high dynamic range images; data hiding; embedding capacity; image quality; pixel saturation; HDR VDP metrics

Citation: Hsieh, K.-S.; Wang, C.-M. Optimal Weighted Modulus: A Secure and Large-Capacity Data-Hiding Algorithm for High Dynamic Range Images. *Electronics* **2024**, *13*, 207. https://doi.org/10.3390/electronics13010207

Academic Editor: Cheonshik Kim

Received: 6 December 2023
Revised: 26 December 2023
Accepted: 29 December 2023
Published: 2 January 2024

1. Introduction

Image data-hiding algorithms [1–4] conceal secret messages within cover images with the aid of stego secret keys, without altering their visual appearance when producing stego images. The images are delivered to the receiver via a public channel, allowing an authorized party to extract secret messages using the same secret stego keys. The data-hiding technique serves as a clandestine communication method, providing a means to transmit sensitive information without arousing the suspicion of adversaries or unauthorized individuals. Image data-hiding offers various applications, including copyright protection, data integrity, non-repudiation, and authentication, among others.

Several image data-hiding algorithms exploiting binary, grayscale, or color images have been investigated in the extant literature [1–5]. Three crucial attributes of image data-hiding techniques are the payload, imperceptibility, and detectability. The payload—that is, the embedding capacity—refers to the number of secret bits that can be embedded in a pixel of the cover image, in bits per pixel (bpp). Imperceptibility represents the ability to distinguish between a cover image and a stego image, which can be assessed by computer analysis. Two common performance measures quantify stego image degradation: the first is peak signal-to-noise ratio (PSNR), for which higher values are better; the second one is the structure similarity index (SSIM), for which larger values are better [6]. Detectability indicates the ability of a data-hiding system to protect the hidden secret message from

being detected by a steganalyzer. In addition, when the features of an image format are altered due to secret message concealment, the data-hiding technique must survive the image format compatibility attacks.

Surprisingly, researchers have paid little consideration to data hiding using high dynamic range (HDR) images [7], even though this type of image offers several advantages over conventional ones. For example, HDR images have an increased color depth and accuracy, allowing an algorithm to capture and display a wider range of colors. In addition, they include a greater range of brightness levels, making them able to exhibit image details in either very bright or dark areas. Finally, HDR imaging, which can capture a greater range of color and brightness values, can render more vibrant and visually plausible images, thus producing scenes similar to human visual perceptions in real life. Due to these benefits, cameras and smartphones even provide applet tools to capture HDR images. Therefore, it is crucial to develop data-hiding algorithms for HDR images, to keep pace with the development of this ever-growing image type.

The current state-of-the-art data-hiding algorithms using HDR images encoded by the RGBE format [8–13] usually exploit homogeneous representation, originally proposed by Yu et al. [9], to conceal secret messages. The RGBE format, detailed in the "real pixel" suggested by Ward in 1991 [14], uses an 8-bit mantissa for each primary and follows it with a single 8-bit exponent. Thus, a pixel in this format contains information in the 32-bit bit pattern, with 8 bits for each primary channel (red, green, blue) and 8 bits for the exponent channel. When increasing by 1 in the exponent channel value, one can halve the three primary color channels to derive similar floating-point values, producing a homogeneous representation with two homogeneity indices; for example, the pixel $P_1(R,\ G,\ B,\ E) = (80,\ 100,\ 140,\ 129)$ has a homogeneous representation $P_2(R,\ G,\ B,\ E) = (40,\ 50,\ 70,\ 130)$ when increasing the exponent from 129 to 130. In this example, exploiting the homogeneous representation (HR) enables a data-hiding algorithm to carry 1 bit of secret message, provided that one has clearly defined in advance the mapping between the exponent values and the secret bits.

The relevant literature has shown that exploiting homogeneous representations to convey secret messages for HDR RGBE images has achieved some success [8–13]. However, this approach suffers from two drawbacks. First, it provides a small embedding capacity, thereby supporting only limited applications because a large portion of pixels in an HDR RGBE image have a zero homogeneity index so are ineligible to carry secret messages. The second disadvantage is more severe, as this approach incurs security concerns. The RGBE image format possesses an important feature: the maximal value in the primary must be greater than or equal to 128, due to the mantissa normalization process [14]. Unfortunately, alteration of an original pixel to its homogeneous representation for message concealment violates this characteristic: $Max(R,\ G,\ B) \geq 128$. Consequently, a steganalysis tool can easily verify the compatibility of the RGBE image format to distinguish between the stego and cover image. This means that asides from successful detection, a steganalyzer can even estimate the length of secret messages carried in a stego image, causing a serious security breakthrough. For example, Tan et al. [15] introduced a steganalyzer to detect HDR steganography, referred to as homogeneous representation-based steganography (HRBS), which can detect a stego image with more than 99% probability.

In this paper, we propose a HDR data-hiding algorithm that can resist the RGBE image compatibility attack, offer a large embedding capacity, and produce stego HDR images with high quality. To provide a large payload, we did not consider the defective homogeneous representation because it is vulnerable to Tan et al.'s steganalytic technique; instead, we modified pixel values in four channels using our proposed optimal weighted modulus (OWM) algorithm for message concealment. In addition, we adjusted pixel values after the message embedding to ensure that the stego image produced complied with the features of the HDR RGBE format. This approach enables our scheme to prevent the steganalytic attack from checking the homogeneity indices to reveal the hidden messages. By changing the embedding parameters, OWM can offer various embedding rates from 3.1699 to 5.7549 bpp.

We cautiously impose a one-way positive change in the exponent channel, thereby reducing as much as possible the impact on the luminance variations caused by message concealment. As a result, our OWM scheme not only offers high embedding rates but also produces high-grade stego HDR images. The tone-mapped image exhibits high PSNR values between 45.05 and 54.49 dB. To remove the security concern, we slightly alter the pixel value to a proper one carefully designed to not compromise the hidden messages. Thus, this approach ensures that the produced stego image is compatible with the RGBE image format, defeating the RGBE image compatibility attack introduced in [15]. The OWM scheme employs an embedding weight to conceal secret messages with the least distortion, so it can also resist the well-known statistical RS steganalysis attack. Finally, we present a shift-embed-confirm (SEC) scheme to resolve the pixel saturation problem when the message concealment produces overflow (>255) or underflow (<0) pixel values. The SEC scheme is so effective that it guarantees avoidance of the pixel saturation problem, even under an intense case where three component channels in the cover pixel contain extreme values.

The primary contribution of our work lies in the proposed OWM scheme, which provides large payloads, produces high-grade stego HDR images, effectively resolves the pixel saturation problem, and offers the feature of undetectability with high security. The comparison results confirm that our scheme outperforms six current state-of-the-art algorithms, making HDR data-hiding more feasible for practical applications.

The rest of this paper is organized as follows. Section 2 surveys the literature related to our work. Our proposed OWM algorithm is detailed in Section 3. Experimental results and discussions are addressed in Section 4, followed by a presentation of the conclusion and suggestions of future work in the Section 5.

2. Related Works

We survey works most related to our proposed algorithm in this section. We will focus on data-hiding algorithms in the literature which make use of RGBE HDR images as carriers to conceal secret messages. For each work being surveyed, we first describe in brief the concept of the algorithm and highlight the embedding capacity the algorithm can offer. We then comment on its detectability, indicating whether it can survive the homogeneous representation steganalysis attack proposed by Tan et al. [15]; their scheme measures changes in the non-zero homogeneity index [9] and then exploits the least squares method to reveal the length of the secret message. This technique can correctly detect the stego image with a probability of over 99% when the length of the embedded secret messages does not exceed 7 bits.

Cheng and Wang [8] pioneered the data-hiding and authentication work for HDR RGBE images. The pixels of an HDR image are classified into a flat area or boundary area according to the exponent channel with respect to the luminance. Then, messages are concealed on the flat area and the boundary area with different strategies. Finally, the reserve areas derived from the flat area are used for embedding authentication information. Their scheme provides for authentication, a large embedding capacity, and limited distortion. Although the embedding rate is in the range of 5.13 to 9.69 bpp, their algorithm pays the expense of producing tone-mapped stego images with small peak signal-to-noise ratios (PSNR) only slightly greater than 30 dB. Their scheme is secure from a cryptographic standpoint and is resistant to brute force attackers. In addition, the hidden messages in the produced stego image are not likely to be detected as the algorithm does not make use of the homogeneous representation for message concealment.

Yu et al. [9] introduced an alternative approach, by modifying a homogeneity index to achieve distortion-free data-hiding in HDR RGBE images. They first defined a homogeneity index for a pixel according to the number of elements in the homogeneous representation group. Next, referring to the homogeneity index, they classified the pixels in an HDR image into a total of five categories: embeddable, promising, singular, null, and neutral. Pixels belonging to the embeddable and promising categories are eligible to embed secret messages. The secret messages are concealed by altering the homogeneity index, which

changes the exponent channel and at the same time modifies the corresponding three primary color channels. Yu et al. [9]. introduced two applications: image annotation and image steganography. For the former, their scheme offers an average embedding rate in the range of 0.12–0.29 bpp; for the latter, it provides an average embedding rate between 0.0010 and 0.0026 bpp. In the image steganography application, the hidden messages can be detected because their scheme makes use of "promising pixels" which violate the RGBE format features.

Wang et al. [10] improved the embedding capacities proposed by Yu et al. [9] and introduced a segment-based method able to make use of all the different pixel expressions in an RGBE image to conceal secret messages. Their scheme first calculates the total homogeneity value that all embeddable pixels can provide. Then, secret messages represented by a binary secret bitstream are segmented into several smaller homogeneity values before concealing them into the corresponding embeddable pixels. Their algorithm offers larger embedding capacities, thereby increasing the embedding rates in the range of 0.00727–0.00778 bpp. However, the hidden messages are detectable because their scheme makes use of homogeneous representations to conceal secret messages, resulting in non-standard HDR RGBE stego images.

Later, Chang et al. [11] further improved the works introduced by Yu et al. [9]. They proposed a modified scheme efficiently taking advantage of all homogeneous representations of each pixel in an HDR image. In addition, they suggested a new homogeneity index table (HIT) to conceal more secret bits for a variety of homogeneity indices. For example, the homogeneity index 6, which cannot be used to convey any secret bit in [9] can now carry 2–3 bits in the new HIT. As a result, their scheme offers an average embedding rate of around 0.1445 bpp, superior to those suggested by Yu et al. [9] and Wang et al. [10]. While Chang et al. [11] improves the embedding capacity, the disadvantage of message detectability remains unsolved.

Tsai et al. [12] introduced a controllable distortion data-hiding scheme and an HDR image authentication technique for HDR RGBE images. A threshold is introduced to exploit as many homogeneous representations as possible in exchange for producing a stego image with controllable and tolerable distortion. Then, an HDR RGBE image is subdivided into several blocks, enabling the embedding algorithm to maximize the number of homogeneous representations to carry more secret messages. In addition, they introduced an authentication algorithm which produces a 128-bit authentication code through homogenous index changes and conceals it using a multiple-base notational system. Their algorithm offers an average embedding rate of 1.07–2.27 bpp, superior to those presented in Chang et al. [11] and Wang et al. [10]. Although Tsai et al.'s method maximizes the number of homogeneous representations, the secret messages can be revealed by checking whether the homogeneity indices have been altered in a stego HDR image.

Chen and Yan [13] proposed an enhanced steganographic scheme, aiming to increase the embedding capacity and improve the security of the work introduced by Yu et al. [9]. The basic idea behind their scheme is that of converting the original pixels which are eligible to convey any secret messages into embeddable pixels in the pre-processing step, thereby increasing the embedding capacities to 0.01–0.026 bpp, around 10 times more than those suggested by Yu et al. [9]. In addition, they introduced a post-processing step which adjusts pixel values to 128 if the maximal value in the red, green, or blue channel is 127. Alternatively, pixels are shifted to 255 or remain at 254, depending on the random bits 0 or 1 generated if the maximal values in the red, green, or blue channel equal 254. In this way, pixels which carry secret messages have the value of 128, 254, or 255. The post-processing step ensures the stego image adheres to the features of the RGBE format, so their scheme can evade detection by steganalytic tools, effectively enhancing the security of embedded messages in HDR RGBE images.

A literature survey indicates that most current state-of-the-art HDR data-hiding algorithms, except [13], exploit homogeneous representations to conceal secret messages. To the best of our knowledge, most previous works [9–12] can be accurately detected by [15] because secret messages are concealed using HRBS. The only exception is [9], which does not exploit the homogeneous representation. Another exception is Chen et al.'s scheme [13] because, although it makes use of a homogeneous representation to embed secret messages, the stego pixel values are adjusted in the post-processing step to satisfy the HDR RGBE format, ensuring $Max(R,\ G,\ B) \geq 128$. Thus, their algorithm avoids the threat of detection. The steganalysis attack aimed at homogeneous representation results in severe security concerns because the resultant stego image fails to satisfy the features of the RGBE format, and thus suffers from risks of being detectable by steganalytic tools. A new data-hiding algorithm for HDR images must resolve this critical problem. In addition, the current state-of-the-art works offer limited embedding capacity because an original HDR image has a limited number of homogeneity indices, making it unable to support various data-hiding applications. In the next section, we introduce our proposed algorithm for dealing with these deficiencies.

3. Our Proposed Algorithm

We describe our proposed optimal weighted modulus (OWM) algorithm in this section; it is undetectable and offers a large embedding payload. Figure 1 shows the flowchart of our scheme for secret message embedding on the sender side and for message extraction by the receiver.

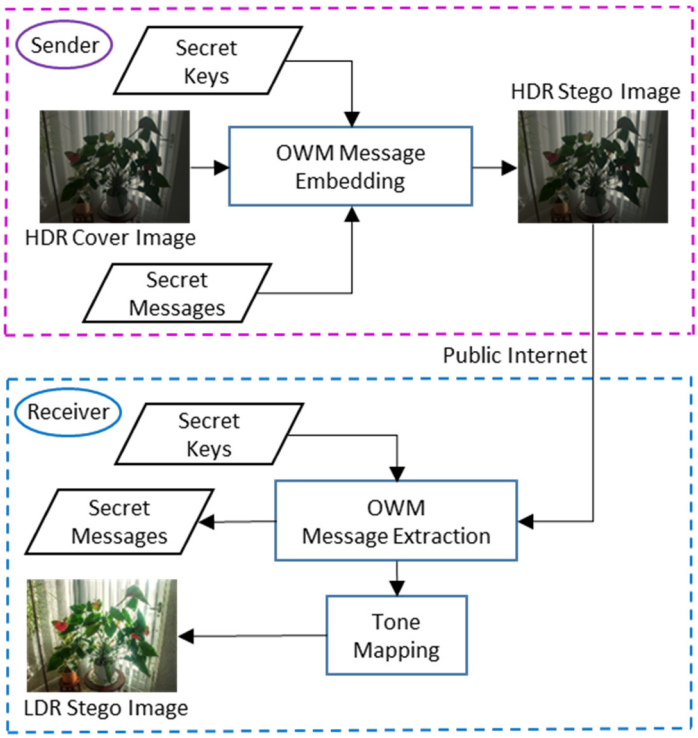

Figure 1. The flowchart of our OWM algorithm for message embedding and extraction.

Our proposed OWM algorithm embeds secret messages using secret keys through the "OWM message embedding process", thereby producing the stego HDR image, which can later be delivered to the receiver side via public Internet without arousing suspicion. This process will be detailed in the embedding algorithm, where the message embedding function contains seven inputs and the output is a stego pixel in an HDR image. The receiver, with the authorized secret keys assigned in advance via a secret channel, can extract secret messages using the "OWM message extraction" process. This porcess is realized by an extraction function, which contains six inputs and which outputs the extracted secret

message. A tone-mapping operator can process the stego HDR image into an LDR stego image for the purpose of visualization. Note that since we directly display the cover HDR image in the input part and the stego HDR image in the output part (without conducting any tone-mapping process), the visualization of these images does not reveal detailed information, in contrast to the tone-mapped LDR stego image, which has a visually plausible appearance.

3.1. Message Embedding Strategy

We consider HDR images encoded by the RGBE format as the secret message carrier because this is one of the most popular formats used in the HDR community. Message embedding in RGBE images differs from that in conventional grayscale or color images because two issues regarding security and luminance must be carefully addressed.

First, the stego image produced must comply with the original RGBE encoding format, to avoid the attack of simple format validation. As described, a pixel in the RGBE format represents a legal pixel if one of the red, green, or blue channels is greater than 128. This feature certifies that a pixel has a single representation. For example, $P = (p_r,\ p_b,\ p_b,\ p_e) = (64,\ 32,\ 140,\ 128)$ represents a legal pixel. However, neither $Q = (32,\ 16,\ 70,\ 129)$ nor $R = (16,\ 8,\ 35,\ 130)$ denote a legal pixel, although they derive the same value as P. To resolve the first issue, we must validate a stego pixel once it has been produced. If pixel validation fails, we need to modify one of channels to ensure a stego pixel represents a legal one, and the distortion caused by such modification must be as small as possible. In this manner, the secret messages can reach a compromise between RGBE format compatibility and stego image quality.

Luminance is the second issue of concern when developing a HDR data-hiding algorithm. HDR images are sensitive to luminance changes because even a subtle change will influence the tone-mapping computing, thereby causing a significant impact on the appearance of the resultant LDR images. To resolve this issue, our OWM scheme restricts the magnitude of change in the exponent channel because it has the largest ramifications. We must ensure that no significant luminance alteration occurs after message concealment. In our scheme, the change in the exponent is in the one-way increased direction and the magnitude is no greater than 1. In other words, $p'_e = p_e$ or $p'_e = p_e + 1$, where p_e and p'_e represent the cover and stego exponent channel, respectively. We remark that the decreased direction in the exponent channel is prohibited because if $p'_e = p_e - 1$, we need to double the values in the three color channels, which may cause pixel overflow if one of the primary color channels in the cover image is greater than 128, as suggested by the RGBE format specification.

3.2. Message Embedding Algorithm

The message embedding in our OWM scheme contains eight parameters, as shown in Algorithm 1. The first parameter I_H represents a cover HDR image encoded by the RGBE format, while the second one K_y portrays the secret key used to determine the embedding path in the message embedding step. In this study, we adopt the random permutation scheme to determine the embedding path [16]. As an example, let $P_1,\ P_2,\ P_3,\ P_4$ represent the original order of pixels in a HDR image I_H. We can use an integer K_y to generate the embedding path $P_3,\ P_1,\ P_4,\ P_2$ so that the first pixel to carry a secret message is P_3 rather than P_1. We hereafter assume that the embedding path has been determined and we focus on message embedding in a pixel $\boldsymbol{P} = (p_r,\ p_b,\ p_b,\ p_e)$ in I_H.

Algorithm 1: Message-Embedding

Input	(1) an HDR RGBE image, I_H; (2) a secret key, K_y; (3) a cover pixel $\boldsymbol{P} = (p_r,\ p_b,\ p_b,\ p_e)$; (4) the channel, $n = 4$; (5) the number system, M; (6) the secret message, d_M; (7) the embedding weight, $\boldsymbol{W}_M^4 = (w_1,\ w_2,\ w_3,\ w_4)$; (8) the vector variation table, $VVT_{\boldsymbol{W}_M^4}$.
Output	a stego pixel $\boldsymbol{P'} = \left(p'_r, p'_g, p'_b, p'_e\right)$.
1	Computing the remainder, $r = \left[\boldsymbol{P}\cdot\boldsymbol{W}_M^4\right]\ mod\ \ M$.
2	Determining the index, $i = (d_M - r)\ mod\ \ M$.
3	Retrieving the row vector, $\boldsymbol{R_i} = VVT_{\boldsymbol{W}_M^4}(i)$, to produce a temporary pixel, $\boldsymbol{P'} = \boldsymbol{P} + \boldsymbol{R_i}$.
4	If the exponent channel is intact $(p'_e = p_e)$, check whether $\boldsymbol{P'}$ represents a valid RGBE pixel (one of $p'_r, p'_g, p'_b \geq 128$).
5	If $\boldsymbol{P'}$ is a valid RGBE pixel, directly output $\boldsymbol{P'}$ as the HDR stego pixel.
6	Else Adjusting components in $\boldsymbol{P'}$ to produce $\boldsymbol{P''}$ which satisfies three conditions:
7	(1) one of $p''_r, p''_g, p''_b \geq 128$;
8	(2) $\left[\boldsymbol{P''}\cdot\boldsymbol{W}_M^4\right]\ mod\ \ M = d_M$;
9	(3) the distortion $\|\boldsymbol{FP''} - \boldsymbol{FP}\|$ is minimal.
10	Output the HDR stego pixel, $\boldsymbol{P''} = \left(p''_r, p''_g, p''_b,\ p'_e\right)$
11	Processing the next cover pixel.
12	If the exponent channel has been changed $(p'_e > p_e)$
13	Deriving $\boldsymbol{P'_a} = \left(\frac{p'_r}{2},\ \frac{p'_g}{2},\ \frac{p'_b}{2},\ p'_e\right)$ using the ceiling function
14	Deriving $\boldsymbol{P'_b} = \left(\frac{p'_r}{2},\ \frac{p'_g}{2},\ \frac{p'_b}{2}, p'_e\right)$ using the floor function
15	Selecting one of them, say $\boldsymbol{P'_k}$, which has smaller distortion, $\|\boldsymbol{FP'} - \boldsymbol{FP'_k}\|$ is minimal
16	Embedding d_M into $\boldsymbol{P'_k}$ again to produce $\boldsymbol{P''} = \left(p''_r, p''_g, p''_b, p''_e\right)$.
17	Adjusting components in $\boldsymbol{P''}$ to produce $\boldsymbol{P'''}$ which satisfies three conditions:
18	(1) one of $p'''_r, p'''_g,\ p'''_b \geq 128$;
19	(2) $\left[\boldsymbol{P'''}\cdot\boldsymbol{W}_M^4\right]\ mod\ M = d_M$;
20	(3) the distortion $\|\boldsymbol{FP'''} - \boldsymbol{FP}\|$ is minimal.
21	Producing the HDR stego pixel, $\boldsymbol{P'''} = \left(p'''_r, p'''_g, p'''_b, p'''_e\right)$.
22	Processing the next cover pixel.

Once the embedding path has been determined, we can convey secret message d_M to a cover pixel $\boldsymbol{P} = (p_r,\ p_b,\ p_b,\ p_e)$ using the embedding weight $\boldsymbol{W}_M^4 = (w_1,\ w_2,\ w_3,\ w_4)$ and the vector varation table $VVT_{\boldsymbol{W}_M^4}$. The output of this algorithm represents the stego pixel $\boldsymbol{P'} = \left(p'_r, p'_g, p'_b, p'_e\right)$. The third parameter n denotes the number of elements used to carry secret messages. We exploit four channels (red, green, blue, and exponent) rather than three channels, leading to $n = 4$. Next, the parameter M indicates the number of secret messages in the M-ary number system that will be carried in n elements. Furthermore, the parameter d_M describes a secret message in the M-ary number system to be carried, $0 \leq d_M < M$. As an example, if the parameter $(n,\ M, d_M) = (4,\ 9,\ 7_9)$, it indicates that a 9-ary secret message 7_9 will be embedded into the pixel $\boldsymbol{P} = (p_r,\ p_b,\ p_b,\ p_e)$.

Next, the sixth parameter $\boldsymbol{W}_M^n$ portrays an n-tuple embedding weight corresponding to the M-ary number system, which can be denoted by $\boldsymbol{W}_M^n = (w_1,\ w_2,\ \ldots,\ w_n)$. This embedding weight will be utilized in the weighted modulus operator to carry the secret message (detailed later). Since we set $n = 4$, the embedding weight is simplified to a 4-tuple vector, $\boldsymbol{W}_M^4 = (w_1,\ w_2,\ w_3,\ w_4)$. Furthermore, the $VVT_{\boldsymbol{W}_M^n}$ represents a vector variation table corresponding to the embedding weight $\boldsymbol{W}_M^n$ that is constructed. This table denotes how to change channels in a pixel $\boldsymbol{P} = (p_r,\ p_b,\ p_b,\ p_e)$ to carry secret messages.

Table 1 shows vector variation tables corresponding to three embedding weights $\boldsymbol{W}_9^4$, $\boldsymbol{W}_{13}^4$, and $\boldsymbol{W}_{15}^4$. The index i is used to retrieve the row vectors $\boldsymbol{R_i}$ via the operator $VVT_{\boldsymbol{W}_M^n}(i)$. For example, if index $i = 5$, the operator $VVT_{\boldsymbol{W}_9^4}(5)$ retrieves the row vector

$\boldsymbol{R_5} = (0, 0, -1, 0)$. See the blue vector shown in the second column in Table 1. As another example, the operator $VVT_{W_{15}^4}(13)$ fetches back the row vector $\boldsymbol{R_{13}} = (1,\ 0,\ 0,\ 1)$. See the green vector shown in the final column of Table 1.

Table 1. Vector variation table corresponding to different embedding weights.

Index ***i***	$\boldsymbol{VVT_{W_9^4}}$ $\boldsymbol{W_9^4}$**=(1, 2, 4, 6)**	$\boldsymbol{VVT_{W_{13}^4}}$ $\boldsymbol{W_{13}^4}$**=(1, 2, 5, 9)**	$\boldsymbol{VVT_{W_{15}^4}}$ $\boldsymbol{W_{15}^4}$**=(1, 5, 11, 12)**
0	(0, 0, 0, 0)	(0, 0, 0, 0)	(0, 0, 0, 0)
1	(1, 0, 0, 0)	(1, 0, 0, 0)	(1, 0, 0, 0)
2	(0, 1, 0, 0)	(0, 1, 0, 0)	(0, 1, 0, 0)
3	(−1, 0, 1, 0)	(0, −1, 1, 0)	(−1, 0, −1, 0)
4	(0, 0, 1, 0)	(−1, 0, 1, 0)	(0, 0, −1, 0)
5	(0, 0, −1, 0)	(0, 0, 1, 0)	(0, 1, 0, 0)
6	(0, 0, 0, 1)	(0, −1, −1, 0)	(0, −1, 1, 0)
7	(0, −1, 0, 0)	(−1, 0, −1, 0)	(0, −1, 0, 1)
8	(−1, 0, 0, 0)	(0, 0, −1, 0)	(0, 0, 1, 1)
9	-	(0, 0, 0, 1)	(−1, −1, 0, 0)
10	-	(−1, −1, 0, 0)	(0, −1, 0, 0)
11	-	(0, −1, 0, 0)	(0, 0, 1, 0)
12	-	(−1, 0, 0, 0)	(0, 0, 0, 1)
13	-	-	(1, 0, 0, 1)
14	-	-	(−1, 0, 0, 0)

The three conditions in lines 7–9 and 18–20 ensure that one of the color components in the red, green, or blue channel is no less than 128, complying with the RGBE encoding. In addition, the second condition ensures that the receiver can correctly extract secret messages. The third condition guarantees that the stego pixel produced has minimal distortion. A stego image thus produced can reach a compromise between image quality and the malicious steganalysis attack.

In lines 9 and 20, ***FP*** represents the floating-point value corresponding to the pixel $\boldsymbol{P}$, which can be derived using Equation (1) [7]. As an example, let $\boldsymbol{P} = (58,\ 129,\ 75,\ 129)$ be a pixel in an HDR image. We can derive $FR = \frac{58+0.5}{256} \times 2^{129-128} = 0.457031$. Similarly, we can compute $FG = 1.011719$ and $FB = 0.589844$:

$$\boldsymbol{FP} = (FR,\ FG,\ FB), \text{ where } \begin{cases} FR = \frac{p_r+0.5}{256} \times 2^{p_e-128} \\ FG = \frac{p_b+0.5}{256} \times 2^{p_e-128} \\ FB = \frac{p_b+0.5}{256} \times 2^{p_e-128} \end{cases}. \tag{1}$$

3.3. An Analysis of Optimal Weight and Computational Complexity

In this section, we analyze the vector variation table to demonstrate that the weights shown in Table 1 are optimal, which means that the message embedding using these weights in our OWM scheme incurs the minimal mean square error, thereby producing high-grade stego HDR images. We consider the case of $(n,\ M) = (4,\ 9)$ and take the embedding weight $\boldsymbol{W_9^4} = (1,\ 2,\ 4,\ 6)$ as an example in our analysis procedure. We remark that the mean square error of this weight is $MSE = \frac{1}{3}$. We prove that an optimal weight must have the same MSE, as detailed below.

First, since we intend to embed a 9-ary secret digit, an optimal weight needs to provide nine patterns of component alterations which have a one-to-one corresponding mapping to nine secret digits, and each pattern must have minimal changes. An optimal weight has four components, so it can provide one pattern where no component has any changes, i.e., (0, 0, 0, 0). Furthermore, an optimal weight needs to provide eight patterns where one of the four components has a single change. This requirement can be derived by the combination expression $C_1^4 \times 2^1$, where 2^1 indicates that the changes can be either *positive* or *negative* in one of the four components, such as (0, 0, 0, ±1), (0, 0, ±1, 0), (0, ±1, 0, 0), or (±1, 0, 0, 0). Thus, an optimal weight offers a total of nine patterns, which

seems to satisfy our requirement. However, since the change in the fourth component (the exponent component) can be in the positive direction, an optimal weight providing the change pattern $(0, 0, 0, -1)$ is ineligible. Thus, an optimal weight needs to provide one more pattern, allowing changes in *two* components. As a result, an optimal weight provides one pattern which has no changes in four components, seven patterns which have single changes in four components, and one pattern which has exactly two changes in four components. Consequently, the mean square error (MSE) of an optimal weight can be derived by MSE $= (1 \times 0 + 7 \times 1 + 1 \times 2)/(9 \times 3) = \frac{1}{3}$. Since the embedding weight $\boldsymbol{W}_9^4 = (1, 2, 4, 6)$ has the same MSE, it is undoubtedly an optimal weight.

We analyze the computational complexity of our algorithm. The message embedding algorithm needs to process every pixel in a HDR image to carry an M-ary secret digit in four channels. The computation includes two modulo operations, checking and possibly adjusting the pixel values to ensure that the feature of $Max(R, G, B) \geq 128$ is satisfied. As a result, the complexity of the message embedding algorithm is $O(N)$. We present two examples using two different secret messages to describe the message embedding algorithm shown in Algorithm 1.

Example 1. *Let* $\boldsymbol{P} = (58, 129, 75, 129)$ *be a cover pixel and the embedding parameters include* $(n, M) = (4, 9)$, $\boldsymbol{W}_9^4 = (1, 2, 4, 6)$, *with the vector variation table* $VVT_{\boldsymbol{W}_9^4}$ *as shown in Table 1. To embed secret message* $d_9 = 6$, *we compute the remainder* $r = \left[\boldsymbol{P} \cdot \boldsymbol{W}_9^4\right] \bmod 9 = 4$. *In line 2, we determine the index* $i = (6 - 4) \bmod 9 = 2$. *In line 3, since the index is* $i = 2$, *we first retrieve the row vector* $\boldsymbol{R_2} = VVT_{\boldsymbol{W}_9^4}(2) = (0, 1, 0, 0)$ *and then produce a temporary stego pixel* $\boldsymbol{P}' = \boldsymbol{P} + \boldsymbol{R_2} = (58, 130, 75, 129)$. *In line 4, since the exponent channel is intact* ($p_e = p'_e = 129$), *we check whether* $\boldsymbol{P}'$ *represents a valid RGBE pixel; namely, one of* $p'_r, p'_g, p'_b \geq 128$. *Since* $p'_g = 130$ *satisfies the requirement, we find that* $\boldsymbol{P}'$ *indeed denotes a valid RGBE pixel. Thus,* $\boldsymbol{P}' = (58, 130, 75, 129)$ *represents the HDR stego pixel.*

Example 2. *Following the embedding parameters used in Example 1, we assume* $\boldsymbol{P} = (107, 242, 58, 129)$ *but adopt a different secret message* $d_9 = 1$ *instead. To embed this secret message, we first compute the remainder* $r = \left[\boldsymbol{P} \cdot \boldsymbol{W}_9^4\right] \bmod 9 = 4$ *and determine the index* $i = (1 - 4) \bmod 9 = 6$. *Thus, we obtain the row vector* $\boldsymbol{R_6} = VVT_{\boldsymbol{W}_9^4}(6) = (0, 0, 0, 1)$ *and produce a temporary stego pixel* $\boldsymbol{P}' = \boldsymbol{P} + \boldsymbol{R_6} = (107, 242, 58, 130)$. *In this example, the exponent channel has been changed from* $p_e = 129$ *to* $p'_e = 130$, *so we follow lines 13–14 and produce* $\boldsymbol{P'_a} = (54, 121, 29, 130)$ *using the ceiling function* $\lceil\ \rceil$ *or* $\boldsymbol{P'_b} = (53, 121, 29, 130)$ *using the floor function* $\lfloor\ \rfloor$. *Next, since* $\boldsymbol{P'_b}$ *has smaller distortion, we adopt it as a new cover pixel. When we embed the secret message again, the new remainder* $r = \left[\boldsymbol{P'_2} \cdot \boldsymbol{W}_9^4\right] \bmod 9 = 3$ *and the index* $i = (1 - 3) \bmod 9 = 7$. *We retrieve the row vector* $\boldsymbol{R_7} = VVT_{\boldsymbol{W}_9^4}(7) = (0, -1, 0, 0)$ *and produce a temporary stego pixel* $\boldsymbol{P}'' = \boldsymbol{P'_2} + \boldsymbol{R_7} = (53, 120, 29, 130)$. *Next, in lines 18–20, we shift the green channel value from* $p''_g = 120$ *to* $p''_g = 129$ *and produce* $\boldsymbol{P}''' = (53, 129, 29, 130)$, *which satisfies all three conditions. Thus,* $\boldsymbol{P}''' = (53, 129, 29, 130)$ *represents the final HDR stego pixel. This example demonstrates that our OWM scheme can conceal secret messages in the exponent channel yet still produce a stego pixel complying with the HDR RGBE encoding.*

3.4. Message Extraction

The message extraction in our OWM algorithm is straightforward, as shown in Algorithm 2. First, the receiver needs to hold the same secret key K_y, so that the extraction path can be determined from the input stego RGBE image I'_H. Since the channel n, the number system M, and the embedding weight $\boldsymbol{W}_M^4$, are available, the secret message concealed in a stego pixel can be extracted using the vector dot as well as the modulus operation. The message extraction algorithm processes every pixel in a HDR image to extract the carried secret message. The algorithm has the complexity of $O(n)$.

Algorithm 2: Message-Extraction

Input	(1) a stego RGBE image, I'_H; (2) a secret key, K_y; (3) a stego pixel $\boldsymbol{P'} = \left(p'_r, p'_g, p'_b, p'_e\right)$; (4) the channel, $n = 4$; (5) the number system, M; (6) the embedding weight, $\boldsymbol{W}_M^4 = (w_1,\ w_2,\ w_3,\ w_4)$;
Output	The secret message, d_M.
1	Using K_y to determine the extraction path within I'_H.
2	Extracting secret message, $d_M = \left[\boldsymbol{P'} \cdot \boldsymbol{W}_M^4\right]\ mod\ \ M$.

Example 3. *We follow the stego pixel produced in Example 1. Without loss of generality, we assume that the extraction path has been determined by K_y in the stego RGBE image I'_H. Let $\boldsymbol{P}^{'} = (58,\ 130,\ 75,\ 129)$ represent a stego pixel and parameters $(n,\ M) = (4,\ 9)$, $\boldsymbol{W}_9^4 = (1,\ 2,\ 4,\ 6)$ are available on the receiver side. Thus, the secret message can be extracted by the modulus operator $d_M = \left[\boldsymbol{P}^{'} \cdot \boldsymbol{W}_M^4\right]\ mod\ M = \left[\boldsymbol{P}^{'} \cdot \boldsymbol{W}_9^4\right]\ mod\ 9 = 6$.*

3.5. Pixel Saturation Solutions

The message concealment will incur distortion in the cover pixel. In our OWM, the maximal change $\|Z\|$ encountered due to message concealment depends on the number of channels n employed to embed the secret message and the number system M used to represent it. In this study, we utilize four channels, leading to $n = 4$. Table 2 shows $\|Z\|$ with respect to different M. Clearly, a larger M will produce a larger $\|Z\|$, which may incur pixel saturation, indicating that channel values are either less than 0 or greater than 255. We remark that since we have regulated the change in the exponent to be less than or equal to 1, the pixel saturation takes place only in three primary color channels: p_r, p_g, and p_b.

Table 2. The values arranged for pixel saturation under different number systems.

Number System, M	**$2 \leq M \leq 57$**	**$58 \leq M \leq 253$**	**$254 \leq M \leq 583$**
Maximal Distortion, $\|Z\|$,	1	2	3
Overflow Value, v_o	254	253	252
Underflow value, v_u	1	2	3

We examine the validity of a HDR stego pixel $\boldsymbol{P'} = \left(p'_r, p'_g, p'_b, p'_e\right)$ once it has been produced. If no pixel saturation occurs, we output $\boldsymbol{P'}$ straightforwardly. If a pixel saturation takes place, we resolve it using our proposed shift-embed-confirm (SEC) scheme. First, we specify which channel, say p_i, suffers pixel saturation. We then shift p_i to v_o or v_u for the overflow or underflow cases, respectively, by referring to $\|Z\|$, as shown in Table 2. Next, we embed secret message d_M using the updated stego pixel $\boldsymbol{P'}$. Finally, we verify the validity of $\boldsymbol{P''}$. If pixel saturation has been eliminated, we output $\boldsymbol{P''}$ directly; otherwise, we repeat the SEC scheme again until no pixel saturation is encountered. We remark that it takes at most two runs of the SEC scheme to produce a pixel-saturation-free stego pixel. We present two examples below to illustrate our SEC scheme.

Example 4. *Assume $\boldsymbol{P} = (58,\ 129,\ 0,\ 129)$; the embedding parameters include $(n,\ M) = (4,\ 13)$, $\boldsymbol{W}_{13}^4 = (1,\ 2,\ 5,\ 9)$ and the vector variation table $VVT_{\boldsymbol{W}_{13}^4}$ as shown in Table 1. Let $d_{13} = 3$ be the secret digit to be conveyed. The message embedding starts by computing the remainder $r = \left[\boldsymbol{P} \cdot \boldsymbol{W}_{13}^4\right]\ mod\ 13 = 8$. Next, we determine the index $i = (3 - 8)\ mod\ 13 = 8$. We first retrieve the row vector $\boldsymbol{R}_8 = VVT_{\boldsymbol{W}_{13}^4}(8) = (0,\ 0, -1,\ 0)$ and then produce a temporary stego pixel $\boldsymbol{P}^{'} = \boldsymbol{P} + \boldsymbol{R}_8 = (58,\ 129,\ 0,\ 129) + (0,\ 0, -1,\ 0) = (58,\ 129, -1,\ 129)$, where an underflow occurs in the blue component p_b. Referring to the SEC scheme, we shift p_b to $v_u = 1$ and update $\boldsymbol{P}^{'} = (58,\ 129,\ 1,\ 129)$. Next, we conceal secret message $d_{13} = 3$ again. Since the new remainder becomes $r = \left[\boldsymbol{P}^{'} \cdot \boldsymbol{W}_{13}^4\right]\ mod\ 13 = 0$ and the index is $i = (3 - 0)\ mod\ 13 = 3$, we retrieve the row vector $\boldsymbol{R}_3 = VVT_{\boldsymbol{W}_{13}^4}(3) = (0, -1,\ 1,\ 0)$, thereby producing the new stego pixel*

$\boldsymbol{P}'' = \boldsymbol{P}' + \boldsymbol{R}_3 = (58, 128, 2, 129)$. *Examining the validity of* $\boldsymbol{P}''$ *shows that no underflow occurs, so we output the HDR stego pixel* $\boldsymbol{P}''$. *We can confirm that a receiver can correctly extract secret message* $d_M = \left[\boldsymbol{P}'' \cdot \boldsymbol{W}_{13}^4\right] \bmod 13 = 3$. *This example shows that our SEC scheme can successfully resolve the pixel saturation problem.*

Example 5. *In this example, we run the SEC scheme twice to eradicate pixel saturation. Assume that a cover pixel contains three extreme values* $\boldsymbol{P} = (255, 255, 255, 129)$, *and the embedding parameters include* $(n, M) = (4, 13)$, $\boldsymbol{W}_{13}^4 = (1, 2, 5, 9)$, *and* $VVT_{\boldsymbol{W}_{13}^4}$ *as shown in Table 1. Assume* $d_{13} = 5$ *represents the secret message. The message embedding starts by computing the remainder* $r = \left[\boldsymbol{P} \cdot \boldsymbol{W}_{13}^4\right] \bmod 13 = 3$. *We determine the index* $i = (5 - 3) \bmod 13 = 2$. *Next, we retrieve the row vector* $\boldsymbol{R}_2 = VVT_{\boldsymbol{W}_{13}^4}(2) = (0, 1, 0, 0)$ *and produce a temporary stego pixel* $\boldsymbol{P}' = \boldsymbol{P} + \boldsymbol{R}_8 = (255, 256, 255, 129)$, *where an overflow occurs in the green component* p_g. *Clearly, we conduct the SEC scheme and shift* p_g *to* $v_o = 254$, *according to Table 2, thereby updating* $\boldsymbol{P}' = (255, 254, 255, 129)$, *and we conceal* $d_{13} = 5$ *again. The new remainder becomes* $r = \left[\boldsymbol{P}' \cdot \boldsymbol{W}_{13}^4\right] \bmod 13 = 1$, *and the index* $i = (5 - 1) \bmod 13 = 4$. *By retrieving the row vector* $\boldsymbol{R}_4 = VVT_{\boldsymbol{W}_{13}^4}(4) = (-1, 0, 1, 0)$, *we produce a new stego pixel* $\boldsymbol{P}'' = \boldsymbol{P}' + \boldsymbol{R}_4 = (254, 254, 256, 129)$. *Unfortunately, the blue component* p_b *encounters an overflow problem. Thus, we conduct the SEC scheme again, where we shift* p_b *to* $v_o = 254$ *before updating* $\boldsymbol{P}'' = (254, 254, 254, 129)$ *accordingly. Once again, we conceal* $d_{13} = 5$. *Finally, we produce a new stego pixel* $\boldsymbol{P}''' = (253, 253, 254, 129)$, *where an overflow has been removed. Apparently, a receiver can extract the correct secret message* $d_M = \left[\boldsymbol{P}''' \cdot \boldsymbol{W}_{13}^4\right] \bmod 13 = 5$. *This example shows that our scheme can effectively terminate the pixel saturation even though a cover pixel contains three extreme values.*

4. Experimental Results and Analysis

We adopt the parameters $(n, M) = (4, 9)$ and $(n, M) = (4, 54)$ using the embedding weights $\boldsymbol{W}_9^4 = (1, 6, 18, 21)$ and $\boldsymbol{W}_{54}^4 = (1, 6, 18, 21)$, respectively, to evaluate twelve HDR RGBE images [17,18]. Table 3 shows the results for message embedding capacities (EC), ranging from 905,901 to 38,711,834 bits for $M = 9$, and 1,644,632 to 70,279,975 bits for $M = 54$. The EC results indicate that our scheme is sufficiently flexible to carry various numbers of secret messages.

Table 3. HDR statistics for the embedding capacity and the mean square error.

				(n, M)=(4, 9)			(n, M)=(4, 54)		
No.	**Image Name**	**Hor.**	**Ver.**	**EC** $(M = 9)$	**FMSE** $(M = 9)$	**Q Value** $(M = 9)$	**EC** $(M = 54)$	**FMSE** $(M = 54)$	**Q Value** $(M = 54)$
1	507	2848	4288	38,711,834	0.6015	9.99882	70,279,975	3.0136	9.99348
2	Anturium	1200	1600	6,086,256	0.5968	9.99984	11,049,384	2.9885	9.99917
3	BenJerrys	2412	4288	32,785,444	0.6004	9.99905	59,520,822	2.9987	9.99481
4	CanadianFalls	2412	4288	32,785,444	0.5950	9.99927	59,520,822	2.9882	9.99609
5	Ceiling	433	660	905,901	0.5803	10.00000	1,644,632	2.9876	9.99998
6	CemeteryTree	2848	4288	38,711,834	0.5895	9.99863	70,279,975	2.9222	9.99300
7	Colorchecker	1312	2000	8,317,883	0.6036	9.99736	15,100,825	3.0823	9.98423
8	Display1000	1536	2048	9,971,722	0.5945	9.99992	18,103,311	2.9768	9.99960
9	Garage	1312	2000	8,317,883	0.6065	10.00000	15,100,825	3.0216	10.00000
10	Kiln	1312	2000	8,317,883	0.6020	10.00000	15,100,825	2.9724	10.00000
11	Sundial	1312	2000	8,317,883	0.5915	9.99996	15,100,825	3.0100	9.99978
12	Windowstar	972	1296	3,993,193	0.5998	9.99992	7,249,501	3.0105	9.99957
Average				16,435,263	0.5968	9.99940	29,837,643	2.9977	9.99664

Table 3 also shows the results of the image quality assessments, which evaluate the distortion between the cover HDR and the stego HDR image. First, we derive the floating-point values in the red, green, and blue channels and compute the floating-point mean

square error (FMSE) between the cover and stego image. For $M = 9$, the average FMSE is small, with an average of 0.5968, and it increases to 2.9977 for $M = 54$. Despite a slight increase in FMSE, the tone-mapped stego HDR images exhibit high-quality stego images (see tone-mapped images shown in Figure 2).

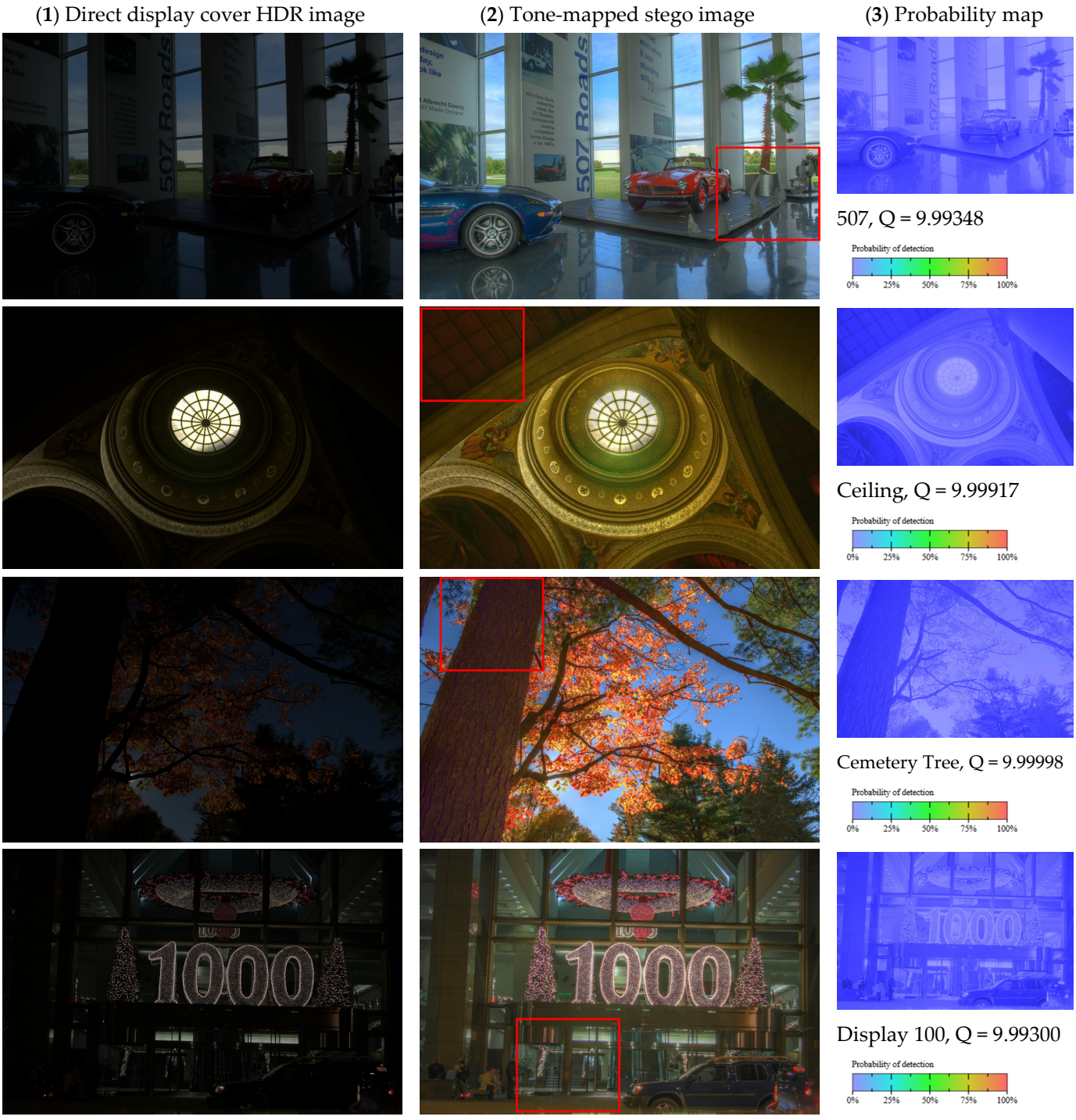

Figure 2. *Cont.*

Figure 2. Six HDR images: (**1**) direct displayed HDR image, first column; (**2**) tone-mapped stego HDR image, second column; (**3**) the probability map image, third column. The blue in the probability map shows a probability of different detection of less than 5% between the cover and stego HDR image.

Next, we present the Q value produced by the HDR-VDP-3 [19–26]; this is a visual metric that can fulfill the full-reference image quality assessment by measuring the test and reference HDR image prior to any tone-mapping processes. The Q value has an upper bound of 10.0 if the test and reference images are so identical that it is almost impossible to distinguish between the test and reference image. Thus, the closer the Q value to its upper bond, the greater the fidelity between the test and reference image. Our experimental results show that the average Q values over twelve HDR test images are 9.99940 and 9.99664 for $M = 9$ and $M = 54$, respectively, and some values even reach the upper bound. The Q values demonstrate that the stego HDR images produced by our scheme exhibit high fidelity between the cover HDR and stego HDR image.

Table 4 shows the results of the image quality assessment (IQA) between the tone-mapped cover and tone-mapped stego images. Note that the stego HDR images are produced using the parameter $(n,\ M) = (4,\ 54)$, and that under this parameter setting, the average embedding capacity is more than 29.8 million bits. Although concealing lots of secret messages, our scheme still produces high-quality stego images, with an average PSNR of 48.05 dB and an average IW-PSNR of 55.0 dB. In addition, the average statistics of the visual saliency-induced index (VSI) [27], SSIM, IW-SSIM [28], and university image quality index (Q-Index) [29] are close to 1.0. All IQA evaluation results demonstrate that despite our scheme conceals lots of secret messgaes, it prouduces high fidelity between the cover and stego image.

Table 4. Statistics for the tone-mapped HDR images $(n,\ M) = (4,\ 54)$.

No.	TM Image	Hor.	Ver.	PSNR	VSI	SSIM	IW-SSIM	IW-PSNR	Q-Index
1	507	2848	4288	47.08	0.999991	0.999908	0.998777	54.02	1.000000
2	Anturium	1200	1600	47.79	0.999991	0.999904	0.999135	55.28	0.999990
3	BenJerrys	2412	4288	47.95	0.999992	0.999942	0.999310	55.51	1.000000
4	CanadianFalls	2412	4288	48.98	0.999886	0.999500	0.999750	52.00	0.999995
5	Ceiling	433	660	45.45	0.999990	0.999946	0.999335	54.30	0.999998
6	CemeteryTree	2848	4288	50.41	0.999995	0.999954	0.999748	59.33	0.999997
7	Colorchecker	1312	2000	49.06	0.999964	0.999808	0.999523	55.69	0.999994
8	Display1000	1536	2048	49.45	0.999988	0.999899	0.999556	56.11	1.000000
9	Garage	1312	2000	45.05	0.999919	0.998683	0.994356	49.24	0.999988
10	Kiln	1312	2000	48.92	0.999984	0.999810	0.999229	56.87	0.999994
11	Sundial	1312	2000	49.84	0.999988	0.999882	0.999468	57.67	1.000000
12	Windowstar	972	1296	46.62	0.999944	0.999588	0.998830	53.95	0.999983
Ave.				48.05	0.999969	0.999735	0.998918	55.00	0.999995

4.1. Visual Perception for Image Assessment

Figure 2 exhibits six test HDR images using the parameters $(n,\ M) = (4,\ 54)$ and $\boldsymbol{W}_{54}^{4} = (1,\ 6,\ 18,\ 21)$. First, we present the images by directly displaying a cover HDR image. Next, we show the stego image after processing the tone-mapping. Finally, we present the probability map.

First, a directly displayed HDR image is not visually pleasant, as the image contains both high and low luminance parts, so it is difficult to delicately exhibit both parts when directly displaying an HDR image. However, the tone-mapped images show visually plausible results, where detailed information can be clearly visualized (for example, inside the red block shown on the image). In this study, we adopted the tone-mapped operator suggested by Mantiuk et al. [30,31]. Since a tone-mapping technique maps the luminance/colors of an HDR image to an LDR image that has the approximate appearance of luminance/colors but a more limited dynamic range, the tone-mapped image can display both high- and low-luminance parts, thus exhibiting subtle image details.

Finally, the probability map produced by the HDR-VDP-3 implies that the detection task imposed by the HDR-VDP-3 predicts a low probability (<5%) of detecting the difference between the cover and stego HDR images. The visual perception and the VDP image assessment demonstrate that our scheme can effectively produce stego HDR images with high quality and visually plausible results.

4.2. RS Steganalysis

Steganalysis intends to detect any hidden message in a stego image. We evaluate the capability of our scheme to resist detection under RS steganalysis [32]. It first derives the number of regular groups (R_M) for the mask $M = [0\ 1\ 1\ 0]$ and (R_{-M}) for the opposite mask $-M = [1\ 0\ 0\ 1]$. The statistical hypothesis of the RS method is that the expected difference of the regular group, $|(R_M - R_{-M})|$, is relatively small in a typical image. The expected difference of the singular group, $|(S_M - S_{-M})|$, has a similar trend. In contrast, if $|(R_M - R_{-M})|$ or $|(S_M - S_{-M})|$ are relatively large, the test image fails to pass the RS detection as it may conceal secret messages. In addition, the RS steganalyzer can estimate the length of a message (in percentage) relative to the resolution of the test image, assuming an embedding rate of 1.0 bpp.

Table 5 shows the RS steganalytic results using tone-mapped HDR image databases, where the cover and stego images are presented for comparison. The red, green, and blue channels are aligned as a one-dimensional channel to derive statistics on regular or singular groups, respectively. In all test stego images, both $|(R_M - R_{-M})|$ and $|(S_M - S_{-M})|$ are relatively small. Referring to the statistical hypothesis, all test stego images pass the RS detection, indicating that the RS steganalyzer is unable to detect any hidden secret messages. In addition, the RS steganalyzer estimates that the length of the secret messages (p)

is relatively small. We remark that the negative values represent one of the solutions in the quadratic equation [32]. The estimation implies that the RS steganalyzer is unqualified to reveal the correct message length, even though our scheme has concealed lots of secret messages.

Table 5. The RS steganalytic results for tone-mapped HDR test images.

		Cover					Stego				
No.	**Image Name**	R_M	R_{-M}	S_M	S_{-M}	$p\times10^{-3}$	R_M	R_{-M}	S_M	S_{-M}	$p\times10^{-3}$
HDR 1	507	0.838	0.846	0.162	0.164	5.1	0.856	0.859	0.144	0.141	6.9
HDR 2	Anturium	0.722	0.726	0.206	0.200	−2.8	0.766	0.768	0.234	0.232	−1.5
HDR 3	BenJerrys	0.726	0.728	0.274	0.272	7.0	0.770	0.771	0.168	0.167	7.6
HDR 4	Canadian Falls	0.775	0.774	0.295	0.296	8.2	0.771	0.774	0.289	0.286	8.6
HDR 5	Ceiling	0.776	0.769	0.167	0.168	5.2	0.804	0.796	0.157	0.153	−6.2
HDR 6	Cemetery Tree	0.653	0.669	0.347	0.341	9.6	0.649	0.665	0.343	0.335	8.7
HDR 7	Colorchecker	0.963	0.959	0.124	0.125	0.3	0.966	0.960	0.134	0.133	7.2
HDR 8	Display1000	0.705	0.714	0.214	0.210	6.9	0.760	0.757	0.240	0.243	1.8
HDR 9	Garage	0.811	0.821	0.189	0.179	−3.1	0.826	0.835	0.174	0.175	6.3
HDR 10	Kiln	0.770	0.773	0.230	0.227	1.2	0.760	0.757	0.240	0.243	1.3
HDR 11	Sundial	0.651	0.650	0.266	0.268	4.8	0.705	0.692	0.295	0.298	9.5
HDR 12	Windowstar	0.716	0.730	0.201	0.199	5.7	0.744	0.723	0.214	0.209	6.8

Figure 3 shows the RS diagram collected from the tone-mapped HDR images "Canadian Falls" and "Ceiling". The RS diagram indicates that the R_M, R_{-M} and S_M, S_{-M} do not reflect significant changes under the increase of secret message concealment from as small as 5% to as large as 100%. Our scheme ensures that the expected values of R_M and S_M equal the value of R_{-M} and S_{-M}, respectively. It can resist the RS analysis attack, as the steganalyzer fails to detect any secret messages hidden within the stego images.

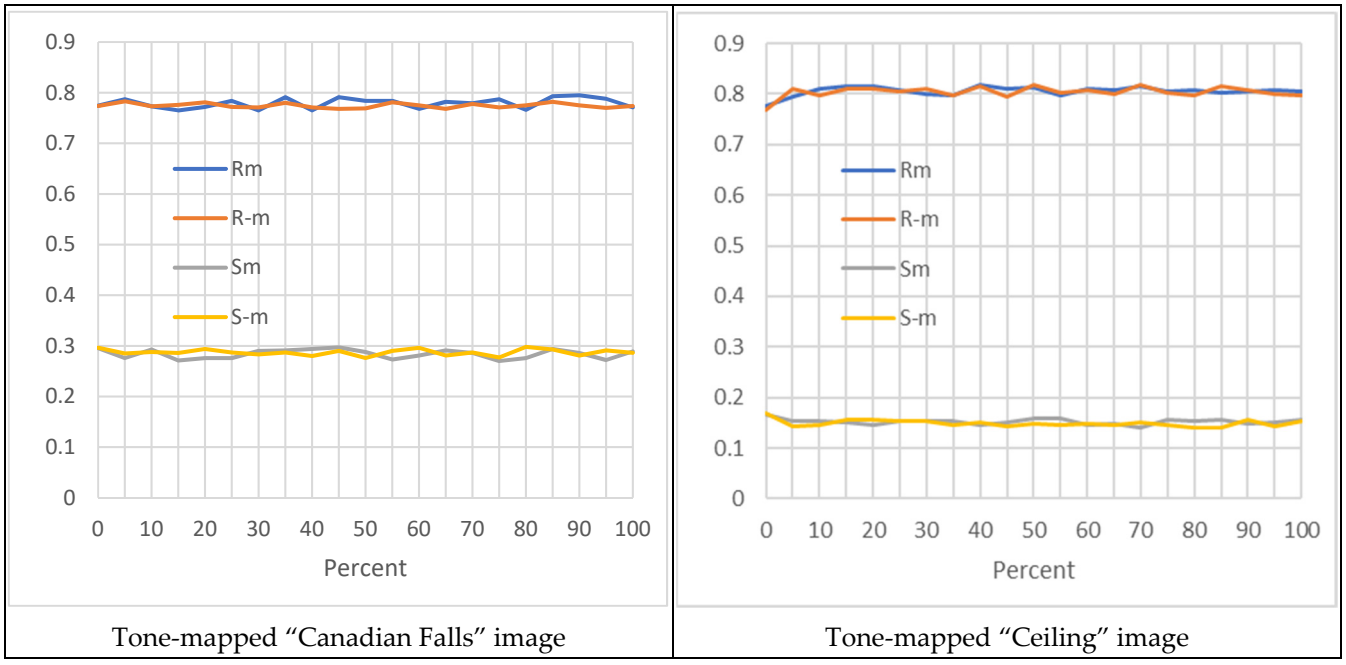

Figure 3. The RS diagrams of the HDR tone-mapped "Canadian Falls" and "Ceiling" images. The x-axis represents the percentage of embedding and the y-axis denotes regular/singular group ratios.

4.3. Comparison with Current State-of-the-Art Works

We compared our OWM algorithm with current state-of-the-art HDR data-hiding schemes, as shown in Table 6. All these methods, from 2009 to 2023, adopt the RGBE encoding in HDR images to conceal secret messages.

Table 6. A comparison with related HDR data-hiding schemes.

Algorithm Comparison	Proposed OWM	Chan & Yan [13]	Tsai et al. [12]	Chang et al. [11]	Wang et al. [10]	Yu et al. [9]	Cheng & Wang [8]
Year	2023	2023	2022	2016	2012	2011	2009
Undetectability	**Yes**	**Yes**	No	No	No	No	**Yes**
RS Steganalysis	**Yes**	No	No	No	No	No	No
ER (bpp)	**3.1699–5.7549**	0.01–0.026	1.07–2.27	0.1391–0.1472	0.1340–0.1373	0.1256–0.1281	5.04–9.70
PSNR (dB)	**45.05–54.49**	51.77–78.60	61.39–75.66	N.A.	N.A.	N.A.	30.00–40.00
SSIM	**0.9991–1.0000**	N.A.	0.9994–0.9999	N.A.	N.A.	N.A.	N.A.

First, the comparison of undetectability evaluates whether a stego image produced by an algorithm carries any hidden messages. We remark that [8] adopted an L-side method, rather than the homogeneous representation, to embed secret messages, thereby achieving greater adaptability and capacity. Since most methods [9–12] exploit homogeneous representations to carry secret messages, they are vulnerable to the steganalysis detection introduced by [15] because the homogeneity indices have been altered. In contrast, our scheme and [13] slightly modify pixel values after message concealment to ensure that the homogeneity indices in the produced stego image remain intact. As a result, our scheme and [13] produce stego images that conform with the original HDR RGBE format, thereby resisting the steganalytic attack.

Next, the RS steganalysis introduced by Fridrich et al. [32] represents a steganalyzer which can reliably and accurately detect least significant bit (LSB) nonsequential embedding in digital images. The RS steganalyzer can effectively detect any stego images using the LSB substitution to carry secret messages, offering an embedding rate of more than 0.05 bits per pixel (bpp). We remark that most methods [8–13] do not conduct experiments for the RS steganalytic attack. In contrast, our method can defeat this attack—even though it offers a large embedding rate of over 0.05 bpp—because while the LSB substitution causes a stationary change in the LSB bit, our scheme alters it with randomness, according to row vectors recorded in the vector variation table.

Third, the embedding rates in bits per pixel (bpp) for these schemes vary, ranging from 0.1340 bpp to as large as 9.70 bpp. While the work introduced by Chen and Wang [8] offers the highest ERs, their scheme produces tone-mapped stego images with rather small PSNR values of 30.0–40.0. In contrast, our OWM scheme offers the second-largest ER (3.1699–5.7549 bpp) and produces a high quality of tone-mapped stego HDR image. We remark that the PSRN and SSIM statistics are duplicated from the published papers; the notation "N.A." denotes that the statistics are not available in the original manuscript.

Finally, the structural similarity index measure (SSIM) [6] is a method for predicting the perceived quality of the digital images. This metric is based on three comparison measurements between the samples of luminance, contrast, and structure. The resultant SSIM index is a decimal value between -1 and 1, where 1 indicates perfect similarity, 0 indicates no similarity, and -1 indicates perfect anti-correlation. We adopt SSIM to measure the similarity between cover and stego HDR images. The SSIM scores produced by our scheme are close to 1.0, outperforming those produced in [12]. The SSIM results demonstrate a high fidelity of the stego image, thanks to the OWM scheme used to conceal secret messages with the minimal mean square error. The comparison concludes that our scheme performs better than six current state-of-the-art HDR data-hiding schemes.

5. Conclusions and Future Work

This paper proposes an optimal weighted modulus algorithm (OWM) to resolve the shortcomings of the current state-of-the-art data-hiding algorithms for high dynamic range images encoded using the RGBE format. Our scheme does not exploit a defective and

vulnerable homogeneous representation to conceal secret messages. Instead, we exploit primary color channels as well as the exponent channel to conceal more secret messages, thereby offering more embedding capacity than counterparts' scales. In addition, we scrupulously regulate the variation in the exponent channel, ensuring that luminance changes due to message concealment are below the pre-designed value. As a result, the average PSNR value collected from the tone-mapped images is larger than 48 dB and the average Q value evaluated from HDR VDP 3.0 is close to the upper bound value, indicating high fidelity to the cover HDR image. Finally, we introduce a shift-embed-confirm (SEC) scheme to solve the pixel overflow or underflow problem, effectively eradicating the pixel saturation despite extreme pixel values. Our OWM scheme adopts an embedding weight and modulus operator to conceal secret messages by referring to the optimal vector variation table, thereby maximally reducing the image distortion.

The experimental results show that OWM can defeat the homogeneous representation attack, where the stego image produced is compatible with the RGBE format. Our scheme is secure under statistical RS steganalytic attacks, surviving malicious eavesdroppers. A comparison result further confirms that our algorithm outperforms six current state-of-the-art schemes. In conclusion, our suggested OWM algorithm successfully enhances the weakness of current state-of-the-art works, extending more HDR data-hiding applications. Future research could consider reversibility issues, to develop reversible HDR data-hiding algorithms and further expand the scope of applications.

Author Contributions: Conceptualization, K.-S.H. and C.-M.W.; methodology, K.-S.H.; software, K.-S.H.; validation, K.-S.H.; writing—original draft preparation, K.-S.H. and C.-M.W.; writing—review and editing, K.-S.H. and C.-M.W.; project administration, C.-M.W.; Supervision, C.-M.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received funding from Ministry of Science and Technology in Taiwan.

Data Availability Statement: Data available in a publicly accessible repository.

Acknowledgments: The authors extend their appreciation to Ministry of Science and Technology in Taiwan for funding this research work under Grant MOST 107-2221-E-005-069, 108-2221-E-005-051, MOST 109-2221-E-005-062, MOST 110-2221-E-005-069, NSC-111-2221-E-005-076, and NSC-112-2221-E-005-072.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Cox, I.J.; Miller, M.L.; Bloom, J.A. *Digital Watermarking and Steganography*, 2nd ed.; Morgan Kaufmann: Burlington, MA, USA, 2008; pp. 425–495.
2. Katzenbeisser, S.; Petitcolas, F. *Information Hiding*; Artech House: Boston, MA, USA, 2016; pp. 1–43.
3. Hussain, M.; Wahab, A.W.A.; Idris, Y.I.B.; Ho, A.T.S.; Jung, K.-H. Image steganography in spatial domain: A survey. *Signal Process. Image Commun.* **2018**, *65*, 46–66. [CrossRef]
4. Subramanian, N.; Elharrouss, O.; Al-maadeed, S.; Bouridane, A. Image steganography: A review of the recent advances. *IEEE Access* **2021**, *9*, 23409–23423. [CrossRef]
5. Liu, J.-C.; Chang, C.-C.; Chang, C.-C.; Xu, S. High-capacity imperceptible data hiding using permutation-based embedding process for IoT security. *Electronics* **2023**, *12*, 4488. [CrossRef]
6. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; Simoncelli, E.P. Image quality assessment: From error visibility to structural similarity. *IEEE Trans. Image Process.* **2004**, *13*, 600–612. [CrossRef] [PubMed]
7. Reinhard, E.; Ward, G.; Pattanaik, S.; Debevec, P.; Heidrich, W.; Myszkowski, K. *High Dynamic Range Imaging, Acquisition, Display, and Image-Based Lighting*, 2nd ed.; Morgan Kaufmann: Burlington, VT, USA, 2010; pp. 85–114.
8. Cheng, Y.-M.; Wang, C.-M. A novel approach to steganography in high-dynamic-range images. *IEEE Multimed.* **2009**, *16*, 70–80. [CrossRef]
9. Yu, C.-M.; Wu, K.-C.; Wang, C.-M. A distortion-free data hiding scheme for high dynamic range images. *Displays* **2011**, *32*, 225–236. [CrossRef]
10. Wang, Z.-H.; Lin, T.-Y.; Chang, C.-C.; Lin, C.-C. A novel distortion-free data hiding scheme for high dynamic range images. In Proceedings of the Fourth International Conference on Digital Home, Guangzhou, China, 23–25 November 2012; pp. 33–38. [CrossRef]

11. Chang, C.-C.; Nguyen, T.-S.; Lin, C.-C. A new distortion-free data embedding scheme for high-dynamic range images. *Multimed. Tools Appl.* **2016**, *75*, 145–163. [CrossRef]
12. Tsai, Y.-Y.; Liu, H.-L.; Ying, C.-Y. Applying homogeneity index modification to high-capacity high-dynamic-range image authentication with distortion tolerance. *Multimed. Tools Appl.* **2022**, *81*, 24957–24976. [CrossRef]
13. Chen, T.-H.; Yan, J.-Y. Enhanced steganography for high dynamic range images with improved security and capacity. *Appl. Sci.* **2023**, *13*, 8865. [CrossRef]
14. Ward, G. Real pixels. In *Graphics Gems II*; Arvo, J., Ed.; Morgan Kaufmann: Burlington, VT, USA, 1991; pp. 80–83. [CrossRef]
15. Tan, L.; Yang, C.; Liu, F.; Luo, X.; Qi, B.; Li, Z. Steganalysis of homogeneous-representation based steganography for high dynamic range images. *Multimed. Tools Appl.* **2020**, *79*, 20079–20105. [CrossRef]
16. Durstenfeld, R. Algorithm 235: Random permutation. *Commun. ACM* **1964**, *7*, 420. [CrossRef]
17. Ward, G. High Dynamic Range Image Examples. Available online: http://www.anyhere.com/gward/hdrenc/pages/originals.html (accessed on 4 December 2023).
18. Munsell Color Science Laboratory HDR Database. Available online: http://www.cis.rit.edu/research/mcsl2/icam/hdr/rit_hdr/ (accessed on 4 December 2023).
19. Aydin, T.O.; Mantiuk, R.; Myszkowski, K.; Seidel, H.-P. Dynamic range independent image quality assessment. *ACM Trans. Graph. (Proc. SIGGRAPH)* **2008**, *27*, 1–10. [CrossRef]
20. Mantiuk, R.; Daly, S.; Kerofsky, L. Display adaptive tone mapping. *ACM Trans. Graph.* **2008**, *27*, 1–10. [CrossRef]
21. Mantiuk, R.; Kim, K.J.; Rempel, A.G.; Heidrich, W. HDR-VDP-2: A calibrated visual metric for visibility and quality predictions in all luminance conditions. *ACM Trans. Graph.* **2011**, *30*, 1–14. [CrossRef]
22. Vangorp, P.; Myszkowski, K.; Graf, E.W.; Mantiuk, R.K. A model of local adaptation. *ACM Trans. Graph.* **2015**, *34*, 1–13. [CrossRef]
23. Mantiuk, R.K.; Ramponi, G. Age-dependent predictor of visibility in complex scenes. *J. Soc. Inf. Disp.* **2018**, *26*, 4–13. [CrossRef]
24. Ye, N.; Wolski, K.; Mantiuk, R.K. Predicting Visible Image Differences Under Varying Display Brightness and Viewing Distance. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019; pp. 5429–5437. [CrossRef]
25. Perez-Ortiz, M.; Mikhailiuk, A.; Zerman, E.; Hulusic, V.; Valenzise, G.; Mantiuk, R.K. From pairwise comparisons and rating to a unified quality scale. *IEEE Trans. Image Process.* **2019**, *29*, 1139–1151. [CrossRef]
26. Mantiuk, R.K.; Hammou, D.; Hanji, P. HDR-VDP-3: A multi-metric for predicting image differences, quality and contrast distortions in high dynamic range and regular content. *arXiv* **2023**, arXiv:2304.13625.
27. Zhang, L.; Shen, Y.; Li, H. VSI: A visual saliency-induced index for perceptual image quality assessment. *IEEE Trans. Image Process.* **2014**, *21*, 4270–4281. [CrossRef]
28. Wang, Z.; Li, Q. Information content weighting for perceptual image quality assessment. *IEEE Trans. Image Process.* **2011**, *20*, 1185–1198. [CrossRef]
29. Wang, Z.; Bovik, A.C. A universal image quality index. *IEEE Signal Process. Lett.* **2002**, *9*, 81–84. [CrossRef]
30. Mantiuk, R.; Myszkowski, K.; Seidel, H.-P. A perceptual framework for contrast processing of high dynamic range images. *ACM Trans. Appl. Percept.* **2006**, *3*, 286–308. [CrossRef]
31. Cerad-Company, X.; Parraga, C.A.; Otazu, X. Which tone-mapping operator is the best? A comparative study of perceptual quality. *J. Opt. Soc. Am. A* **2018**, *35*, 626–638. [CrossRef] [PubMed]
32. Fridrich, J.; Goljan, M.; Du, R. Detecting LSB steganography in color, and gray-scale images. *IEEE MultiMedia* **2001**, *8*, 22–28. [CrossRef]