applied sciences

MDPI

Article

Enhanced Steganography for High Dynamic Range Images with Improved Security and Capacity

Tzung-Her Chen * and Jing-Ya Yan

Department of Computer Science and Information Engineering, National Chiayi University, Chiayi City 600, Taiwan; yan0983007@gmail.com
* Correspondence: thchen@mail.ncyu.edu.tw

Abstract: High-dynamic-range (HDR) images are widely regarded as the ideal format for digital images due to their ability to accurately render a wider range of luminance values. Recently, research has focused on introducing data-hiding techniques to HDR images, but these studies often suffer from a low hiding capacity. In 2011, a steganography scheme was proposed, which utilizes homogeneity in RGBE (red, green, blue, and exponent) format, a popular HDR format, and results in cover images with only slight and ignorable distortions after embedding. However, the capacity of the scheme is limited, and their steganography process may raise suspicions due to the abnormal distribution of pixel values caused by the multiplication and division in the embedding process. There is no denying that security is always the main concern for steganography. A major potential problem became clear after a careful revisiting of the scheme. This paper presents an enhanced steganography scheme that improves embedding capacity by modifying non-embeddable pixels to become embeddable in cover images and avoids potential security weaknesses by using additional random numbers to alter pixel values. The proposed scheme improves the embedding capacity of HDR images while maintaining their visual quality and security against statistical analysis attacks. The experimental result shows that the capacity increases 10 times without visual distortion.

Keywords: high dynamic range (HDR); steganography; RGBE; steganalysis

Citation: Chen, T.-H.; Yan, J.-Y. Enhanced Steganography for High Dynamic Range Images with Improved Security and Capacity. *Appl. Sci.* **2023**, *13*, 8865. https://doi.org/10.3390/app13158865

Academic Editor: Mostafa Fouda

Received: 23 April 2023
Revised: 21 July 2023
Accepted: 22 July 2023
Published: 1 August 2023

1. Introduction

With the increasing prevalence of the Internet, the security of communication channels cannot be guaranteed due to the risk of eavesdropping. In cases where transmitted data is confidential, such as military intelligence or medical histories, encryption is a common method used to protect sensitive information. However, encrypted data is often more easily detected by eavesdroppers due to its complex nature compared to unencrypted data. Consequently, steganography [1–4] has emerged as a crucial technique for enhancing information security.

Steganography, in contrast to cryptography, is concerned with concealing communication [5]. The digital objects typically used in information security include images, texts, videos, and others. Among these, digital images are frequently employed due to their redundancy and ubiquitous use in daily life. The resulting images after secret data is embedded are known as stego-images, while those without such data are called cover images. The evaluation of a steganography technique involves three primary benchmarks: the capacity to conceal secret data, the visual quality of the stego-images, and the security, which refers to the detection of steganalysis [2]. A steganography scheme should therefore aim to maximize the amount of data that can be embedded in stego-images while minimizing the distortion between cover images and stego-images and avoiding suspicion of the presence of any secret information. Recently, there has been a growing interest in deep learning-based image steganography techniques, and this has involved discussions on existing methods and has provided valuable insight [3].

With advances in imaging technology, higher-quality images that better resemble real-world scenes are being sought after. This has led to the development of a new format for digital images, which can be divided into two categories: low-dynamic-range (LDR) images and high-dynamic-range (HDR) images. An LDR image is a traditional image that is composed of three color channels, red (R), green (G), and blue (B), each represented using 8 bits, for a total of 24 bits. In contrast, an HDR image represents each R, G, or B channel using 32 bits, for a total of 96 bits. Unlike LDR images, the dynamic range of HDR images can be recorded using 96 bits, providing greater detail in even the darkest and brightest regions beyond what the human eye can perceive. HDR images can be generated using HDR cameras or by combining multiple LDR images with different exposures [6]. Due to the high cost of storing and transmitting 96-bit HDR images, researchers have developed various compact formats for HDR images, including RGBE [7], LogLuv [8], OpenEXR [9], and JPEG-XT [10].

While steganography schemes for LDR images have reached relative maturity, the research on steganography for HDR images is still in its early stages. HDR imaging techniques have been developed to capture the full range of color and light that the human eye can perceive in the real world. As a result, HDR media contain significantly richer content than their LDR counterparts and are therefore much more valuable. In fact, most cameras and smartphones currently available on the market are capable of capturing HDR images. Thus, it is crucial to develop proper tools for protecting the intellectual property of digital HDR media from the early stages of technology development.

There are two primary categories of data hiding or steganography algorithms designed for HDR images. The first type aims to achieve high-capacity data hiding [11,12] by conveying a significant amount of secret messages, but at the expense of producing a stego-image with substantial distortion. These algorithms are currently state-of-the-art and offer an embedding rate of at least 5 bits per pixel. The second type of algorithm aims to achieve a high image quality in data hiding [4,13–17]. These algorithms leverage the RGBE HDR encoding format to conceal a small quantity of messages; however, the capacity provided by these algorithms is limited to less than 0.5 bits per pixel. They are also known as distortion-free algorithms since any distortion produced after secret message embedding is negligible, resulting in a stego-image that is identical to the cover tone-mapped image after the tone-mapping operation. Due to the limited capacity offered by these distortion-free algorithms, it becomes challenging for them to support applications that require a large capacity.

Wang et al. [11] were among the pioneers to propose an HDR steganographic algorithm that conceals secret messages inside images in the Radiance RGBE format without impairing the image quality, making it undetectable to potential attackers. Yu and Wang [18] proposed a different approach for steganography in HDR images in RGBE format, leveraging the characteristics of the format to separate flat and boundary areas in cover images and embed data using two-side methods [19] with different strategies. Li et al. [12] introduced a data hiding scheme for HDR images in LogLuv format, which involves embedding data in the least significant bit (LSB) of the HDR image. The core of Li et al.'s method is inspired by the optimal pixel adjustment process (OPAP) [20,21], which adjusts pixel values to minimize pixel variation after LSB replacement. However, most of the aforementioned research modifies steganography techniques originally designed for LDR images to apply to HDR images, rather than developing tailored approaches for HDR image formats.

In a recent study, Yu et al. [13] presented a data-hiding approach for HDR images in the RGBE format, which can be used for image annotation or steganography. The scheme proposed by Yu et al. leverages the homogeneity present in the RGBE format to embed secret data. Building upon this work, Chang et al. [14] (2016) proposed a novel data-hiding scheme for image annotation application by utilizing homogeneous representation groups more efficiently. However, it is noteworthy that potential vulnerabilities may exist in Yu et al.'s data-hiding scheme when applied for steganography purposes.

A. Motivation

This research is centered around the steganography scheme proposed by Yu et al. [13], which has an average capacity within the range of 0.0010–0.0026 bits per pixel. In order to fully leverage the strengths of Yu et al.'s scheme tailored for HDR images, it is worth exploring potential methods of enhancing its capacity and security for steganography purposes. Our findings reveal that, while Yu et al.'s scheme maintains imperceptibility in pixel differences before and after embedding, it suffers from a scarcity of embeddable pixels in general HDR images, potentially resulting in low capacity. Additionally, the embedding process disrupts the normal distribution of pixel values, which introduces potential weaknesses when stego-images are subjected to statistical analysis attacks. Thus, a potential security concern exists.

B. Main Contributions

This paper presents an improved steganography scheme for HDR images that are encoded with the RGBE format. The scheme builds upon the distortion-free steganography scheme proposed by Yu et al., which is thoroughly analyzed in this paper. Although Yu et al.'s scheme exhibits imperceptible changes in pixel differences before and after embedding, the scheme's embeddable pixels are scarce for general HDR images. This is due to the low capacity of the scheme and the disruption of number distribution during the embedding process, making stego-images vulnerable to statistical analysis attacks.

To address these limitations, the proposed scheme employs pre-processing to convert the original pixels into embeddable pixels, thereby increasing the number of embeddable pixels. Additionally, post-processing is designed to eliminate abnormal number distributions by incorporating random numbers and addressing potential security vulnerabilities arising from statistical analysis. The primary contribution of this study lies in the proposed scheme, which not only builds upon the strengths of Yu et al.'s scheme but also significantly improves the embedding capacity of HDR images. Simultaneously, the proposed scheme ensures the preservation of visual quality and reinforces security against statistical analysis attacks. The experimental result shows that the capacity increases 10 times without visual distortion.

The rest of this paper is organized as follows. Section 2 briefly introduces the related work including Yu et al.'s scheme and its potential weaknesses. The enhanced steganography scheme is proposed in Section 3. Experimental results and discussions are shown in Section 4, which is followed by the conclusion in Section 5.

2. Preliminary

This section provides a brief overview of the scheme proposed by Yu et al. [13], followed by an analysis of its potential weaknesses with respect to steganography security and hiding capacity.

2.1. Embedding in Yu et al.'s Scheme

The RGBE format, also known as the Radiance format, was introduced by Ward [7] in 1991 as the first efficient HDR image format. This format utilizes 32 bits to represent each pixel in an HDR image, which is more efficient compared to the uncompressed HDR image format that requires 96 bits. In the raw HDR image format, each pixel comprises three color channels: red, green, and blue, and each channel is represented by a 32-bit floating-point value. However, in RGBE images, each pixel consists of four channels to capture the red, green, blue, and exponent values. These channels are represented by 8-bit integers, and their values range from 0 to 255.

In the context of HDR image processing, we denote a pixel of raw HDR images as $P(r, g, b)$, whereas a pixel that has been encoded with the RGBE format is represented as $P(R, G, B, E)$. The transformation of pixel values from the raw HDR format to the RGBE format can be achieved using the methods described in Equations (1) and (2).

$$E = \lceil \log_2[\max(r, g, b)] + 128 \rceil \quad (1)$$

$$r = \left\lfloor (256 \times R) / \left(2^{E-128}\right) \right\rfloor,\ g = \left\lfloor (256 \times G) / \left(2^{E-128}\right) \right\rfloor,\ b = \left\lfloor (256 \times B) / \left(2^{E-128}\right) \right\rfloor \quad (2)$$

Due to the exponent channel in the RGBE format, multiple representations exist to express the color of a pixel. Specifically, a pixel $P(R, G, B, E)$ can also be represented as $P'(2R, 2G, 2B, E-1)$ (or $P''(\frac{R}{2}, \frac{G}{2}, \frac{B}{2}, E+1)$) by multiplying (or dividing) each color channel by 2 and subtracting (or adding) 1 in the exponent channel. This feature is referred to as the homogeneity of RGBE, as defined by Yu et al. [13].

To facilitate comprehension, an illustrative example is presented to explicate the embedding operations described below.

Example 1. *Table 1 presents the homogeneous representation group (HRG_p) elements of a pixel $P(48, 80, 44, 127)$, which includes $P(48, 80, 44, 127)$, $P'(24, 40, 22, 128)$, and $P''(12, 20, 11, 129)$ sorted in ascending order of homogeneity, as determined by the exponent channel values. The number of elements in HRG_p is equivalent to the homogeneity value (HV_p), while each element is assigned a homogeneity index (HI_p). It should be noted that the element $(12, 20, 11, 129)$ exhibits an odd value of 11 in the blue channel, rendering the division operation inapplicable and thus classifying it as the dominant channel for P.*

Table 1. Homogeneity of RGBE: an example of pixel $P(48, 80, 44, 127)$.

Pixel P	HV_p	HRG_p	HI_p
$P(48, 80, 44, 127)$	3	(48,80,44,127)	0
		(24,40,22,128)	1
		(12,20,11,129)	2

To illustrate the embedding operations in Yu et al.'s scheme in a generalized manner, we present the following example. Specifically, Table 2 is employed to embed the corresponding secret bits into a cover pixel with varying homogeneity values. Building upon the example provided in Table 1, we first compute the HV_p and HI_p values of cover pixel $P(48, 80, 44, 127)$. Since the HV value of pixel P is 3, Table 2 is consulted to determine that one bit can be conveyed. Assuming a secret bit of 0 is to be embedded, Table 2 indicates an HI value of 1, resulting in the modification of $P(48, 80, 44, 127)$ to $P'(24, 40, 22, 128)$, as depicted in Table 1. Conversely, if the embedding secret bit is 1, the corresponding HI value is 0, and $P(48, 80, 44, 127)$ remains unchanged.

Table 2. Homogeneity index table.

Number of Bits Conveyed	HV	HI						
		0	1	2	3	4	5	6
0	1	NP *						
1	2	"0"	"1"					
1	3	"1"	"0"	NA **				
2	4	"00"	"01"	"10"	"11"			
2	5	"01"	"10"	"11"	"00"	NA		
2	6	"10"	"11"	"00"	"01"	NA	NA	
2	7	"11"	"00"	"01"	"10"	NA	NA	NA

* "NP" means that it is not possible to embed the secret message if HV = 1. ** "NA" means that no bit pattern is assigned.

Yu et al. proposed a classification method for pixels, dividing them into seven distinct categories, as presented in Table 3. Here, the variable $\max(R, G, B)$ denotes the highest value present in a given pixel. Based on their characteristics, pixels are further classified into either "*regular*" or "*irregular*" categories. The "*regular*" category indicates that the highest value of a pixel across the three channels, denoted as $\max(R, G, B)$, is equal to or greater than 128, while the "*irregular*" category refers to $\max(R, G, B)$ being less than 127. Importantly, a pixel can only belong to one of these two categories, but not both.

For a comprehensive understanding of Yu et al.'s scheme, readers are referred to the original paper.

Table 3. The categories of pixels in an HDR image encoded by the RGBE format.

Pixel Category	Satisfied Condition
Regular	$\max(R, G, B) \geq 128$
Irregular	$\max(R, G, B) \leq 127$
Embeddable	$2 \leq HV_p \leq 7$
Promising	$\max(R, G, B) = 127\ (HV_p = 2)$ $\max(R, G, B) = 254\ R, G, B\ \in even\ (HV_p = 2)$
Singular	$HV_p = 1$
Null	$R = G = B = 0\ (HV_p > 8)$
Neutral	$HV_p = 8$

2.2. Security by Statistical Analysis

The scheme proposed by Yu et al. serves the dual purpose of image annotation and image steganography. In the context of steganography, the primary objective is to ensure security against statistical analysis. As in the case of cryptography, steganography algorithms are assumed to be publicly available, and the security of the scheme is based on the concealment of secret data without detection. If it can be demonstrated that an algorithm can determine, with a higher success rate than random guessing, whether a given image contains embedded secret data, then the steganography scheme is deemed to have been compromised.

Steganalysis, akin to cryptanalysis in cryptography, involves identifying concealed messages that have been concealed through steganography using various techniques, including perceptual, statistical, specific, and universal blind analysis [22]. While Yu et al. have shown promising results in perceptual analysis, which pertains to the level of distortion, their scheme has a clear vulnerability in specific analysis. The specific analysis concentrates on identifying weaknesses in a particular steganography scheme. While Yu et al. have asserted that stego-HDR-images do not arouse suspicion among eavesdroppers, our findings demonstrate that this claim is not always valid.

Artificial Distribution of Pixels' Values

Two categories of pixels are identified (see Table 3) as suitable for the embedding of secret messages based on the following definitions [13]: *embeddable* and *promising*.

$$P(R, G, B, E)\ is \begin{cases} embeddalbe,\ 2 \leq HV_p \leq 7 \\ promising, \begin{cases} \max(R, G, B) = 127\ and\ HV_p = 2 \\ \max(R, G, B) = 254,\ R, G, B\ \in even\ and\ HV_p = 2 \end{cases} \end{cases} \quad (3)$$

In the context of the "*embeddable*" category, a pixel is considered *embeddable* if its HV value falls within the range from 2 to 7. An *embeddable* pixel may also be designated as "*promising*", which can be further divided into two specific categories. The first category corresponds to pixels with a maximum value of 127 in any of the Red, Green, or Blue channels, while the second category requires that the maximum value be 254 and that all three channel values be even. Specifically, the first category of "*promising*" pixels with

$\max(R, G, B) = 127$ can facilitate one multiplication operation, while the second category with $\max(R, G, B) = 254$ can facilitate one division operation. Therefore, the "*promising*" pixels with an HV value of 2 ($HV_p = 2$) have the ability to convey one bit of a secret message.

Yu et al.'s image steganography scheme employs the technique of utilizing "*promising*" pixels to conceal secret messages, thereby ensuring that the magnitude of change resulting from embedding the secret data remains within a reasonable range in each case. However, upon conducting a detailed analysis, two potential vulnerabilities have been identified in Yu et al.'s steganography approach.

Observation 1. *The proportion of even-valued integers present in the three color channels where* $max(R, G, B) = 254$ *will be altered from 25% to 12.5% following the embedding procedure in Ref. [13].*

As noted in Ref. [13], the capacity is primarily attributable to pixels with a homogeneity value of 2. These pixels make up roughly 11% of the pixels. Thus, it can be inferred that the majority of almost embeddable pixels possess an HV of 2. As only "*promising*" pixels are selected for embedding secret messages in steganography, it is important to note that these pixels possess certain characteristics, namely HV = 2 and $\max(R, G, B) = 254$ or $\max(R, G, B) = 127$. In order to examine homogeneity, the following analysis is presented. With the exception where $\max(R, G, B) = 254$ or $\max(R, G, B) = 127$, the other four values contain at least two even numbers, which can be combined to generate another element through a division by 2 or multiplication by 2 of another element. The remaining two numbers have a 50% probability of being even.

In summary, in the three color channels of embeddable pixels, the likelihood of an arbitrary number's being even is 75%, while the likelihood of it's being odd is 25%. Prior to message embedding, the probability that all three color channels are even in the cover image is 25% (i.e., $\frac{1}{2} \times \frac{1}{2} \times 100\%$). However, after embedding the secret message, approximately half of the even numbers will become odd due to multiplication and division, resulting in a probability of 12.5% that all three color channels are even in the stego-images, illustrated in Figure 1.

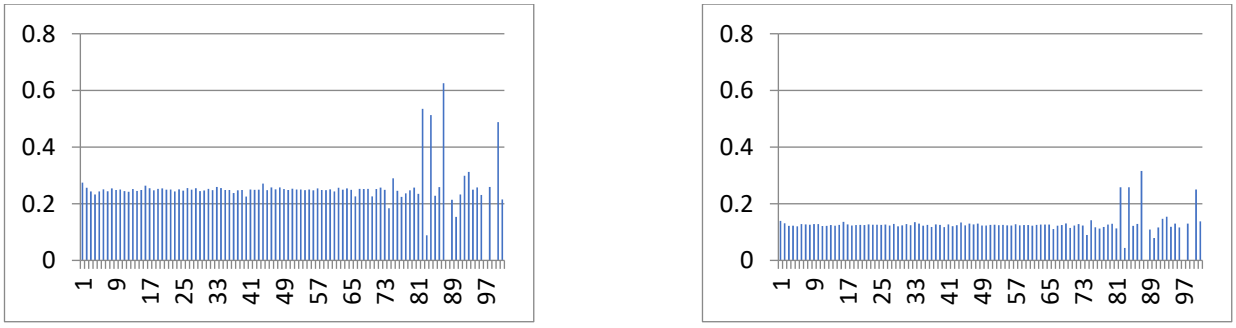
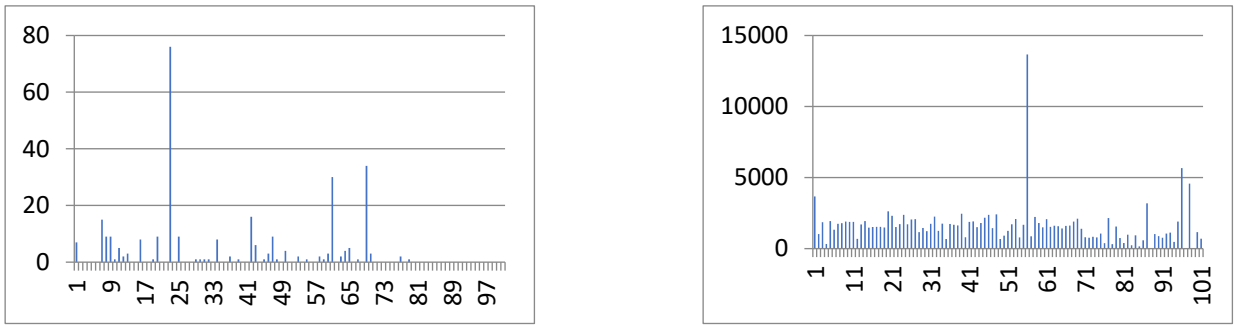


Figure 1. The probability histograms of 101 HDR images, wherein the three color channels of each pixel possess even values: (**a**) 0.25 of the original cover images and (**b**) 0.125 of the embedded images, as per Yu et al.'s scheme.

Observation 2. *The number of embeddable "irregular" pixels noticeably increases following the embedding procedure in Ref. [13].*

Based on the analysis of the HDR image database in the study by Yu et al., the number of embeddable "*irregular*" pixels is typically negligible. However, following the embedding process, the number of embeddable "*irregular*" pixels noticeably increases. This operation disrupts the typical distribution, as roughly half of the "*promising*" pixels in each HDR image are transformed into embeddable "*irregular*" pixels. As shown in Figure 2, these non-normal distributions of pixel counts can easily trigger suspicion upon a specific analysis of the stego-image. The above analysis is presented in Section 4.



(**a**) (**b**)

Figure 2. The histograms are the number of embeddable "irregular" pixels in 101 HDR images. (**a**) The cover images and (**b**) the embedded images, as per Yu et al.'s scheme.

As the eavesdropper acquires an increasing number of HDR images, the vulnerability of the security scheme to specific forms of analysis becomes increasingly evident.

2.3. Hiding Capacity

In the context of image steganography and image annotation applications, the concealment capacity is consistently regarded as a critical factor. The experimental findings in Yu et al.'s image steganography reveal a small capacity ranging from 0.0010 to 0.0026 bits per pixel (bpp). However, this level of capacity is not considered outstanding.

In summary, there are two key challenges that require addressing: (1) security, i.e., the need to mitigate abnormal distribution of data, and (2) capacity, i.e., the requirement to enhance the embedding performance.

3. Proposed Scheme

To address the aforementioned issues, an improved steganography scheme composed of three phases is presented. The corresponding flowchart is depicted in Figure 3. The proposed approach involves three phases: pre-processing, embedding, and post-processing. In the pre-processing phase, the original cover image undergoes modification to generate additional pixels with homogeneity values, increasing embeddable pixel capacity. The subsequent embedding phase entails the incorporation of secret data into the cover image. In the post-processing phase, a pseudo-random number generator (PRNG) generates a random bit stream, which is utilized to adjust the pixel values of the embedded image, resulting in a stego-image with a histogram similar to that of typical natural images.

Phase 1: Pre-Processing

The statistical analysis conducted prior to embedding reveals that, with the exception of 0, the maximum value of the three color channels for most pixels is not less than 127. This finding indicates that the maximum pixel value cannot be divided more than once. To address this limitation, the proposed scheme assumes that the embeddable pixels can be divided or multiplied once for each of the three color channels while increasing the exponent channel by 1. To implement this assumption, we propose a straightforward scheme that involves two steps.

First, we identify specific pixels using one of four cases. Second, we adjust the pixel values using one of four different methods, depending on the case. These two steps are further elaborated below.

Step 1. The pixels with $\max(R, G, B) = 127||128||254||255$, where $||$ means the *or* operation, are selected.

Step 2. The selected pixels are further modified as follows.

Case 1: If a pixel with $\max(R, G, B) = 127$, the individual R, G, and B values of the pixel are unaltered.

Case 2: If a pixel with $\max(R, G, B) = 128$, the maximum value, i.e., 128, undergoes a decrement of 1, and the new maximum value becomes 127.

Case 3: If a pixel with $\max(R, G, B) = 254$, the odd pixel values can be converted to even values by subtracting 1.

Case 4: If a pixel with $\max(R, G, B) = 255$, either the maximum value of 255 or any odd values will decrease by one to become even values.

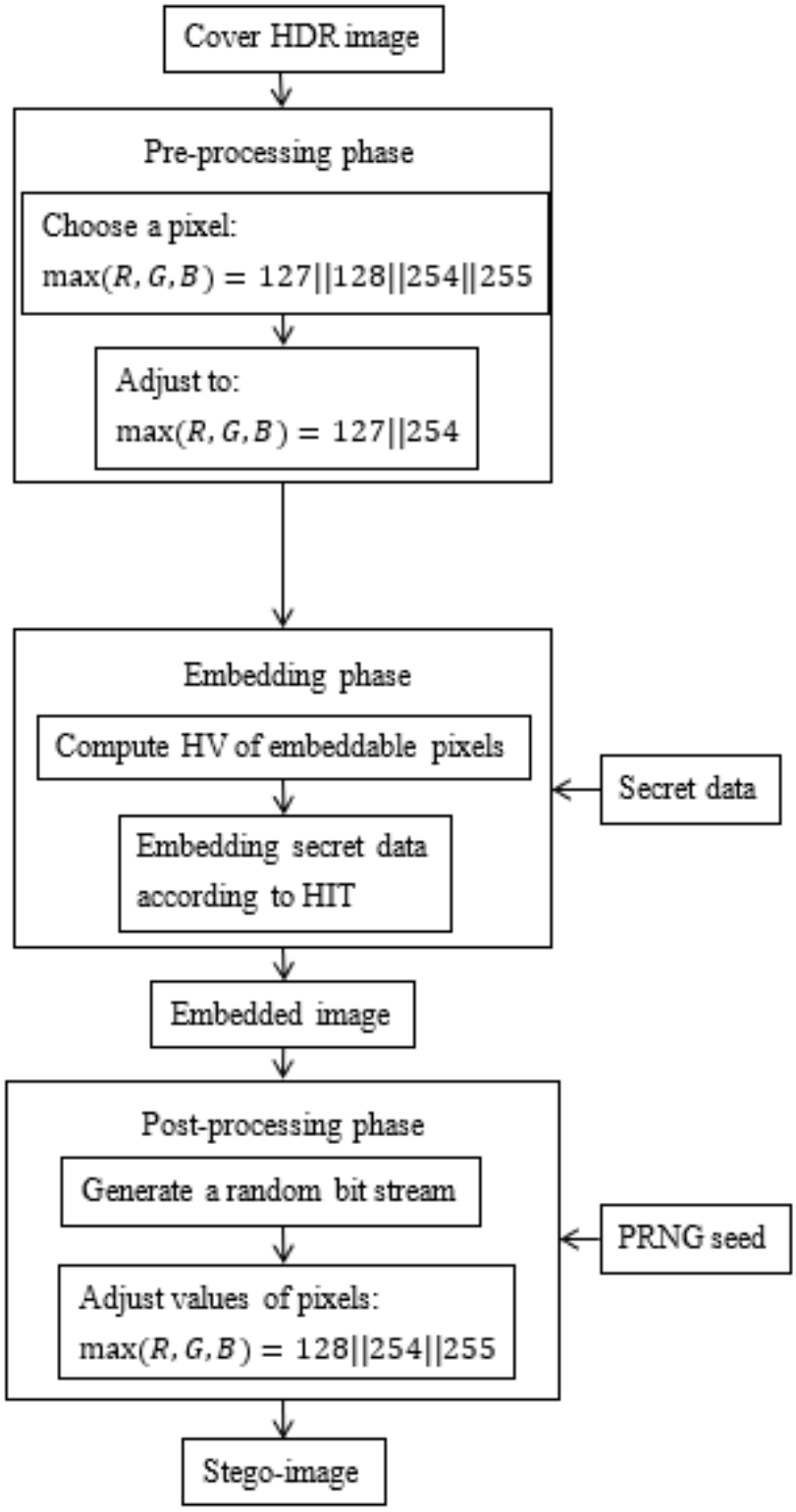


Figure 3. The flowchart of the proposed steganography scheme.

Phase 2: Embedding

The embedding procedures are analogous to those delineated in Yu et al.'s scheme and, accordingly, are briefly introduced below.

Step 1. For a $P(R, G, B, E)$ in RGBE format, its homogeneous representation group (HRG_P) elements are determined, and its corresponding homogeneity value (HV_p) for this pixel is defined as the number of elements in the homogeneous representation group.
Step 2. Every element in the HRG is sorted according to the value represented in the exponent channel in ascending order, and an index is assigned to each sorted element. This enables the definition of a homogeneity index (HI) for every sorted element in HRG, with the HI_P having a range from 0 to (HV_p-1).
Step 3. Upon determining the homogeneous group and the homogeneity value of a pixel K, HV_K, the pixel capacity in bits is computed, denoted as C_K, as shown in Equation (4).

$$C_K = \lfloor \log_2 HV_K \rfloor \quad (4)$$

Step 4. The homogeneity index table (Table 2) is utilized to facilitate the embedding process of the cover pixel $K(R, G, B, E)$. Depending on its homogeneity value HV_K, the numbers of bits that can be conveyed are listed in the first column of Table 2. In the third column, the bit patterns of the secret message that can be concealed, corresponding to different homogeneity indices, are described. By referring to Table 2, the cover status C(HV_K, HI_K) can be modified, and the status of the cover pixel, which is changed to the stego status S(HV_K, HI'_K), is recorded. This indicates that a desired bit pattern of the secret message has been conveyed by the stego pixel. If the homogeneity value (HV_K) is less than or equal to 1, this pixel cannot convey any secret message.

Phase 3: Post-Processing

Once the embedding process of our enhanced scheme is completed, the resulting embedded image exhibits a concentration of pixel values towards even numbers. To address this, we perform a further adjustment to transform the embedded images into stego-images that exhibit a normal distribution of numbers across the three color channels. This is achieved through the following two-step process. Firstly, a PRNG is employed to generate a randomly arranged bitstream. Secondly, for each of the three color channels, a random bit is selected and mapped to a corresponding number. While this process may lead to increased image distortion, it is an acceptable trade-off to achieve a higher level of security, as the eavesdropper is unable to obtain the original or cover images. Moreover, the distortion introduced by our scheme is imperceptible to the human eye. The aforementioned two steps are further elaborated below.

Step 1. A random bit stream is generated by a pseudo-random number generator.
Step 2. Pixel values are modified according to the following cases.

Case 1: Given a pixel with $\max(R, G, B) = 127$, the maximum values are increased by adding 1 to become 128.

Case 2: Given a pixel with $\max(R, G, B) = 254$, if the corresponding randomly generated bit is "0", the maximum value remains unchanged. However, if the bit is "1", the maximum value is incremented by 1 to become 255. Similarly, the values of the remaining two color channels are modified based on their respective randomly generated bits. If a bit is "1", the value remains the same. It is worth noting that the maximum value of the embedded image is limited to 254 to avoid overflow during post-processing.

The secret message extraction process is made straightforward. A stego HDR image is provided, and every pixel is examined. The homogeneity value, HV_K, for each stego pixel (e.g., K) that is inspected, is computed. If HV_K is less than or equal to 1, no secret message is conveyed by this pixel. Alternatively, if HV_K is greater than 1, the homogeneous representation group, HRG_K, for this stego pixel is produced, and the number of concealed secret message bits in the cover pixel K is calculated using Equation (3). The homogeneity index of the cover pixel, HI_K, is determined by comparing the cover pixel K with all elements in HRG_K, and the status of the stego pixel, S(HV_K, HI'_K), is generated. Ultimately,

by referring to the homogeneity index table (Table 2) and $S(HV_K, HI'_K)$, the bits of the secret message can be extracted.

4. Experimental Results and Discussions

In this section, the positive experimental results that support the contention in this paper are provided. The experiments were conducted on a dataset of 101 HDR images, as described in [23,24].

4.1. Distribution of Numbers

The scheme is initially evaluated by analyzing the rate of even numbers in RBGE-format stego-images. The proportion of pixel values in which all three color channels are even numbers is depicted in Figure 4. The results illustrate that the histogram in Figure 4b obtained from the stego-image using Yu et al.'s scheme significantly deviates from that in Figure 4a of the original cover image. Conversely, the histogram in Figure 4c derived from the proposed scheme still maintains a resemblance to that in Figure 4a.

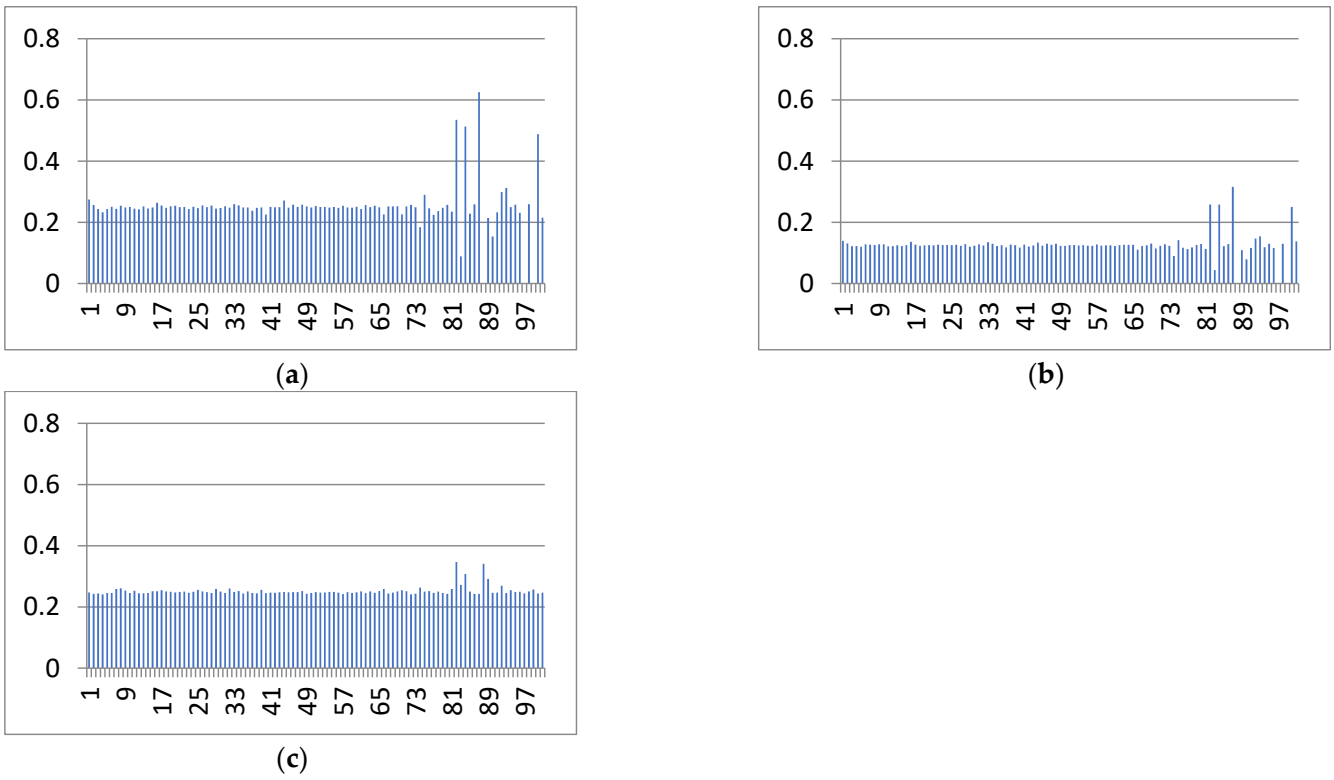


Figure 4. The proportion of pixel values in which all three color channels are even numbers. (**a**) The histograms of original cover HDR images, (**b**) the histograms of stego-HDR-images in Yu et al.'s scheme, and (**c**) the histograms of stego-HDR-images in the proposed scheme.

The embedding process proposed by Yu et al. results in an increase in the number of embeddable "*irregular*" pixels, as demonstrated in Figure 5a, despite the fact that the rate of such pixels is close to zero. Specifically, Yu et al.'s embedding operation disrupts the general pixel distribution by converting half of the "*promising*" pixels in each HDR image into embeddable "*irregular*" pixels. In contrast, the proposed scheme eliminates this potential weakness, as illustrated in Figure 5b.

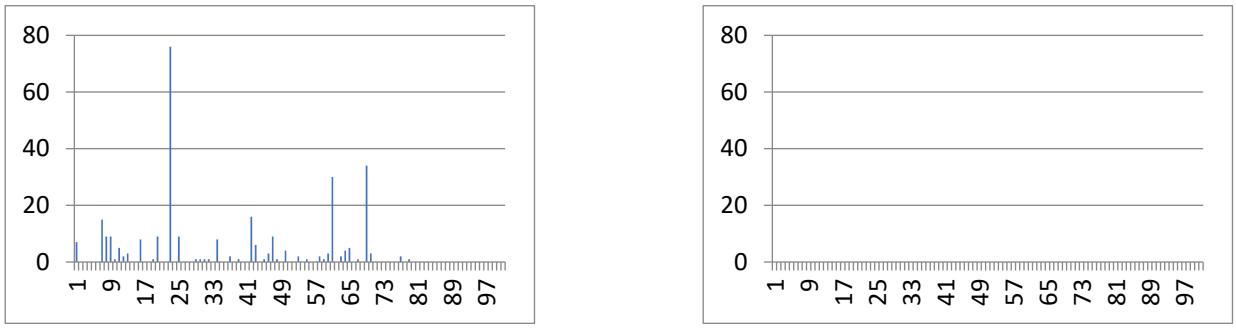


Figure 5. The occurrence rate of "irregular" pixels of $\max(R, G, B) = 127$ (**a**) in Yu et al.'s scheme, and (**b**) in the proposed scheme.

4.2. Improvement of Capacity

Figure 6 presents a comparison of capacity between Yu et al.'s scheme and the improved scheme proposed in this paper. The results demonstrate a significant increase in average capacity by a factor of 10. The experimental findings of the proposed image steganography reveal a capacity improved by 0.0080–0.0420 bits per pixel (bpp).

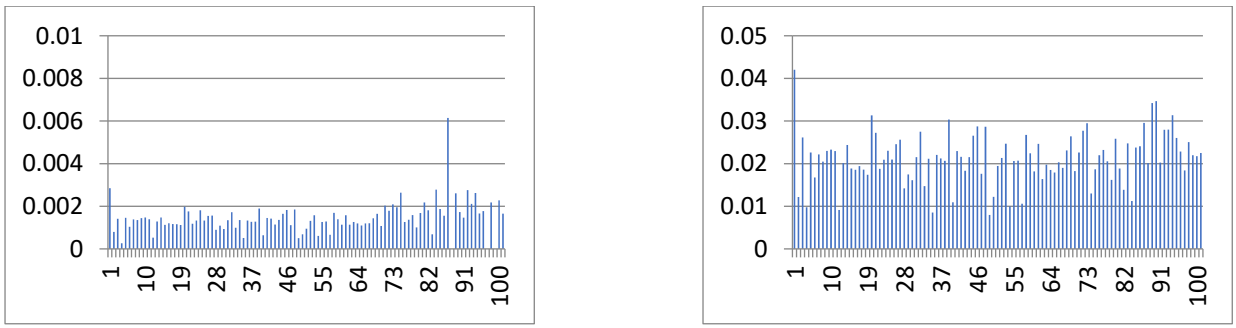


Figure 6. The comparison of capacity between Yu et al.'s scheme (**left**) and the enhanced scheme proposed in this paper (**right**).

As HDR images cannot be accurately displayed on conventional monitors, in Figure 2, we present stego-images that have been processed using a tone mapping operator (TMO) to convert the HDR images into LDR images. The first column shows the original images without any secret image embedding, while the second and third columns display the stego-images embedded using Yu et al.'s scheme and the enhanced scheme proposed in this paper, respectively.

The peak signal-to-noise ratio (*PSNR*) analysis is a common analysis of LDR image authentication schemes and is defined as

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \text{ (dB) } and$$

$$MSE = \frac{1}{3 \times M \times M} \sum_{k \in \{R,G,B\}} \sum_{i=1}^{M} \sum_{j=1}^{M} \left(I_{i,j}^{k} - \tilde{I}_{i,j}^{k} \right)^2.$$

where $I_{i,j}^{k}$ and $\tilde{I}_{i,j}^{k}$ are the original image and the embedded version. The larger the *PSNR*, the better the quality of the image.

The *PSNR* values are provided below the images in the second and third columns. The *PSNR* values for the enhanced scheme are lower than those for Yu et al.'s scheme, indicating that our scheme has greater distortion. However, the *PSNR* value in the range of 51.77–78.60 is acceptable and greater than 30, as shown in Figure 7. This level of distortion is typically imperceptible to the human eye.

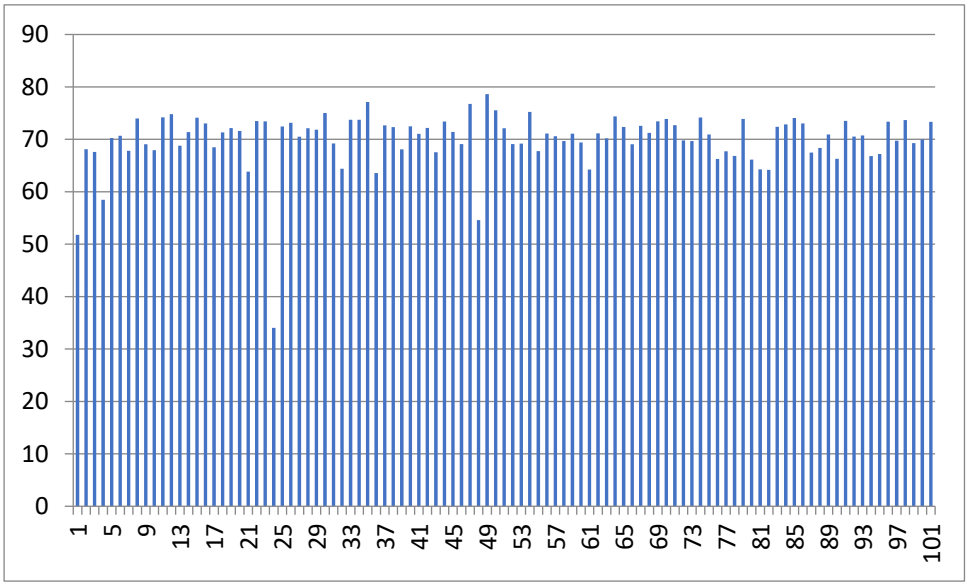


Figure 7. The *PSNR* values of stego-images with tone mapping.

Due to space constraints, one HDR image was randomly chosen from a set of 101 images to serve as an illustrative example (Figure 8a). The resulting steganographic image (Figure 8b) achieved a *PSNR* value of 72.66, demonstrating an excellent preservation of image quality. Moreover, its capacity of 0.0212 greatly surpasses the capacity of 0.0013 achieved in the prior study [13].

(**a**) (**b**)

Figure 8. Experimental results of the image "display1000": (**a**) The cover image. (**b**) The embedded image by the proposed scheme with *PSNR* = 72.66 and enhanced capacity = 0.0212 (the original capacity = 0.0013) [13].

According to the experimental findings, among the 101 HDR images examined, three images were found to lack "*promising*" pixels for embedding the secret message by Yu et al.'s scheme. This limitation is not present in the proposed enhanced scheme.

5. Conclusions

The proposed enhanced steganography scheme addresses the limitations of Yu et al.'s approach. By modifying non-embeddable pixels and introducing additional randomization, the scheme significantly improves the embedding capacity of HDR images without compromising their visual quality. Furthermore, the enhanced scheme mitigates potential security weaknesses that could arise from abnormal pixel value distributions. It is worth emphasizing that security remains the primary concern in steganography, and the proposed scheme effectively enhances the security of embedded messages in HDR images.

The substantial increase in embedding capacity achieved by the enhanced scheme opens up new possibilities for information hiding in HDR images. Future research could focus on further optimizing the scheme's performance and evaluating its robustness against a wider range of attacks.

Author Contributions: Conceptualization, T.-H.C.; Methodology, T.-H.C. and J.-Y.Y.; Software, J.-Y.Y.; Formal analysis, T.-H.C.; Investigation, T.-H.C.; Writing—original draft, J.-Y.Y.; Writing—review & editing, T.-H.C.; Supervision, T.-H.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Ministry of Science and Technology of Taiwan under grant MOST 110-2221-E-415-006-MY2 and the National Science and Technology Council of Taiwan under grant NSTC 112-2221-E-415-005.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Anderson, R.J.; Petitcolas, F.A.P. On the limits of steganography. *IEEE J. Sel. Areas Commun.* **1998**, *16*, 474–481. [CrossRef]
2. Abdulla, A.A.; Sellahewa, H.; Jassim, S.A. Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images. *Multimed. Tools Appl.* **2019**, *78*, 17799–17823. [CrossRef]
3. Kumar, V.; Sharma, S.; Kumar, C.; Sahu, A.K. Latest trends in deep learning techniques for image steganography. *Int. J. Digit. Crime Forensics (IJDCF)* **2023**, *15*, 1–14. [CrossRef]
4. Khudhair, S.K.; Sahu, M.; KR, R.; Sahu, A.K. Secure Reversible Data Hiding Using Block-Wise Histogram Shifting. *Electronics* **2023**, *12*, 1222. [CrossRef]
5. Fridrich, J.; Goljan, M.; Du, R. Detecting LSB steganography in color and gray-scale images. *IEEE Multimed.* **2001**, *8*, 22–28. [CrossRef]
6. Debevec, P.E.; Malik, J. Recovering high dynamic range radiance maps from photographs. *Proc. SIGGRAPH* **1997**, *1997*, 369–378.
7. Ward, G. Real pixels. *Graph. Gems II* **1991**, *2*, 80–83.
8. Larson, G.W. LogLuv encoding for full-gamut, high-dynamic range images. *J. Graph. Tools* **1998**, *3*, 15–31. [CrossRef]
9. Industrial Light & Magic, OpenEXR. 2013. Available online: http://www.openexr.org (accessed on 3 July 2021).
10. Richter, T.; Artusi, A.; Ebrahimi, T. JPEG XT: A new family of JPEG backward-compatible standards. *IEEE MultiMed.* **2016**, *23*, 80–88. [CrossRef]
11. Wang, C.M.; Cheng, Y.M.; Tzeng, Y.P.; Kan, H.W.; Huang, Y.H.; Leu, P.Y.; Hsieh, Y.S. A novel data hiding algorithm for HDR images based on a modified side match scheme. *J. Eng. Natl. Chung Hsing Univ.* **2005**, *16*, 209–220.
12. Li, M.T.; Huang, N.C.; Wang, C.M. A data hiding scheme for high dynamic range images. *Int. J. Innov. Comput. Inf. Control.* **2011**, *7*, 2021–2035.
13. 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]
14. Chang, C.C.; Nguen, 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]
15. Chang, C.C.; Nguyen, T.S.; Lin, C.C. Distortion-free data embedding scheme for high dynamic range images. *J. Electron. Sci. Technol.* **2013**, *11*, 20–26. [CrossRef]
16. Wang, Z.H.; Chang, C.C.; Lin, T.Y.; Lin, C.C. A novel distortion-free data hiding scheme for high dynamic range images. In Proceedings of the 2012 Fourth International Conference on Digital Home, Guangzhou, China, 23–25 November 2012; pp. 33–38.
17. Lan, C.F.; Wang, C.M.; Lin, W. XtoE: A Novel Constructive and Camouflaged Adaptive Data Hiding and Image Encryption Scheme for High Dynamic Range Images. *Appl. Sci.* **2022**, *12*, 12856. [CrossRef]
18. Cheng, Y.M.; Wang, C.M. A Novel Approach to Steganography in High-dynamic Range Images. *IEEE MultiMed.* **2009**, *16*, 70–80. [CrossRef]
19. Chang, C.C.; Tseng, H.W. A steganography method for digital images using side match. *Pattern Recognit. Lett.* **2004**, *25*, 1431–1437. [CrossRef]
20. Chan, C.K.; Cheng, L.M. Hiding data in images by simple LSB substitution. *Pattern Recognit.* **2004**, *37*, 469–474. [CrossRef]
21. Wu, H.C.; Wu, N.I.; Tsai, C.S.; Hwang, M.S. Image steganography scheme based on pixel-value differencing and LSB replacement methods. *IEEE Proc. Vis. Image Signal Process.* **2005**, *152*, 611–615. [CrossRef]
22. Fridrich, J.; Goljan, M. Practical steganalysis of digital images-state of the art. In *Proceedings of SPIE 4675, Security and Watermarking of Multimedia Contents IV*; IEEE Computer Society: Washington, DC, USA, 2002; Volume 4675, pp. 1–13.

23. High Dynamic Range Image Examples. Available online: http://www.anyhere.com/gward/hdrenc/pages/originals.html (accessed on 3 July 2021).
24. Munsell Color Science Laboratory HDR Database. Available online: http://www.cis.rit.edu/research/mcsl2/icam/hdr/rit_hdr/ (accessed on 3 July 2021).