cryptography

MDPI

Article

Algorithm of Information Embedding into Digital Images Based on the Chinese Remainder Theorem for Data Security

Oleg Evsutin [1,2,*] and Kristina Dzhanashia [1]

[1] Department of Cyber-Physical Systems Information Security, HSE Tikhonov Moscow Institute of Electronics and Mathematics, National Research University Higher School of Economics, 123458 Moscow, Russia; kmdzhanashia@edu.hse.ru

[2] Laboratory of Cyber-Physical Systems, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, 117997 Moscow, Russia

* Correspondence: evsutin.oo@gmail.com

Received: 18 October 2020; Accepted: 3 December 2020; Published: 6 December 2020

Abstract: With the huge transfers of data involved in the modern world, it is both crucial and challenging to maintain the security of data. This paper proposes a novel algorithm of information embedding into digital images that could be used to protect confidential information. The presented algorithm makes use of the Chinese remainder theorem and adaptive embedding to achieve good imperceptibility along with the possibility of hiding a decent amount of confidential information. The algorithm is evaluated via computing experiments and evaluation results, as well as comparison with similar works, demonstrate good imperceptibility qualities of the proposed scheme.

Keywords: data security; information hiding; digital images; Chinese remainder theorem

1. Introduction

The last few years witnessed an increased interest in information security. Effective security requires protection of all systems involved including applications, clouds, end devices, gateways, etc. In the modern world, a huge amount of data is constantly being transferred, which makes securing these data a challenging task. With data transfers happening in multiple spheres of life, including healthcare and social interactions, people's safety and privacy could be in danger if data are not protected properly. As presented in Figure 1, typically data travels through end devices, the Internet and a cloud; moreover, data can also travel among various end devices [1]. While it is important to protect data on the end devices, it is equally important to protect it during data exchange. One of the ways to secure data is to hide it. The huge amount of data exchanged nowadays adds additional obscurity to the already hidden data, thus further complicating the task of protected data presence detection and data infiltration. To hide data an information embedding algorithm can be applied. The algorithm can be used along with more conventional information protection techniques such as cryptography to create more secure systems. A few particular applications that use embedding methods to achieve security will be discussed in the following sections of this work.

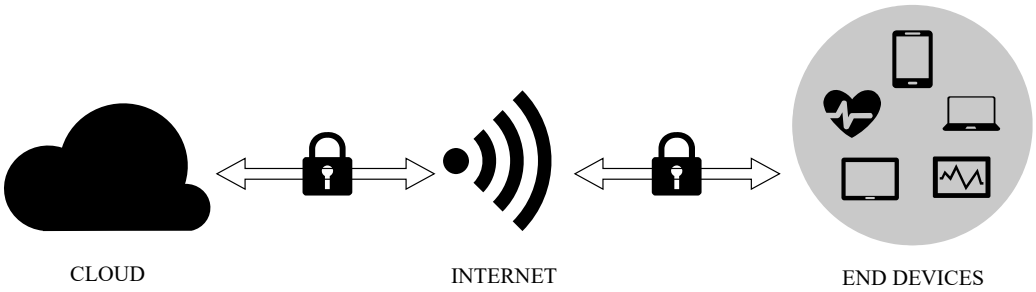

Figure 1. Typical data transfers.

The process of data hiding using an information embedding algorithm can be described as follows. The media data that are used as inconspicuous objects is called cover media. Using an algorithm and a key the secret message is embedded in the cover media. The cover media with a secret message is transferred through the channel. At this stage, the object that contains secret information should be indistinguishable from ordinary objects. When the media reaches its destination, the secret message is extracted from it using the algorithm and the key. However, there may not always be an option to safely transfer additional information such as the key. In other cases, the additional security in form of an information hiding key may not be required. This work proposes the method that does not depend on any information besides the algorithm itself and the length of the transferred message. The latter could be arranged to be a fixed value as it is most often possible to lengthen the message to a given bigger size.

All information embedding algorithms try to obtain three main qualities, imperceptibility, capacity, and robustness against various cover processing attacks. This is a complicated task as these qualities contend with each other. Imperceptibility refers to the third party's inability to discover embedded information, capacity to the amount of information that can be covered in the cover without damaging it, and robustness to the amount and type of medium modifications that a message can withstand.

Different types of media can serve as cover objects including digital audio, video, and images. Digital images tend to have high redundancy, availability, and popularity [2]. Those features facilitate the task of information hiding. This work focuses exclusively on digital images.

Information embedding into digital images can be performed either in spatial or in the transform domain. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) are some of the most widespread choices for transform domain techniques. DFT is a window transformation. It is usually applied independently to separated parts of a cover image. This could lead to appearance of notable boundaries among separated parts and visual quality deterioration of a cover image. DCT is a special case of DFT; however, it is less computationally expensive. The third most widespread transform in digital image processing is DWT. DWT refers to a family of transformations with varying properties. When compared to DFT and DCT, DWT has advantage of not being a window transform; thus, during the embedding process in image's frequency domain the image does not split into separated parts. Moreover, even if embedding artifacts are visible, they are still smoother than when using DFT or DCT.

The present study focuses on enhancing the effectiveness of information embedding into digital images that could be used to improve data security. The main contribution of the present study is as follows:

- A novel ternary logic-based technique of information embedding into digital objects is proposed. The technique allows reducing the number of changes in a digital image that are required to embed a message of a given length. This feature leads to improved effectiveness of the information embedding.
- A novel ternary logic and the Chinese remainder theorem-based algorithm of information embedding is proposed. The ternary logic is implemented through the Chinese remainder

theorem. Moreover, the Chinese remainder theorem enables rigorous mathematical tools of the number theory to be used in the task of information embedding effectiveness enhancement. The most prominent features of the proposed algorithm are imperceptibility qualities and an option not to transfer any side information.

- Multiple applications of information embedding techniques are analyzed. The most suitable application for the proposed technique is suggested.

The rest of the paper is organized as follows. The review of related works is presented in Section 2. In Section 3, the proposed information embedding algorithm is described. An experimental evaluation of the algorithm is presented in Section 4. Finally, the discussion and conclusion are given in Sections 5 and 6.

2. Related Works

A large body of literature on data security and information embedding provides a basis for the present study.

Although the art of hiding information in inconspicuous objects has been practiced for a long time, its modern and scientific formulation is often considered to be introduced by Simmons through the "Prisoners Problem" [3]. Anderson and Petitcolas [4] adopt the aforementioned "Prisoners Problem" in work that provides a deep insight into information hiding theory. The article presents the unified terminology on the subject and discusses the main obstacles in the information hiding field. Ultimately, the authors demonstrate the advantages of using pixels blocks parity in the embedding process. Despite the fact that the work presents a comprehensive theory overview, it does not focus on more particular questions such as media types. The more practical introduction to the information concealment in digital media is provided by Johnson and Jajodia [5]. The authors present a brief history of the subject and give an overview of the most prominent issues concerning digital images steganography such as image formats and common approaches to information hiding. Steganography is a term used for a type of covert communication that works by hiding secret messages in inconspicuous objects that are sent to the intended destination. The relatively up-to-date steganography techniques survey is presented in [2].

The aforementioned works provide an overview of the subject while the following ones present some information hiding methods. Data concealment methods often manipulate the least significant bits (LSBs) in images to embed data imperceptibly. In [6], LSB substitution based spatial domain steganography is applied to the medical images. Contrary to LSB techniques, the intermediate significant bit substitution is used in [7]. The latter technique is reversible meaning that the cover image can be restored at the receiver side. In [8], the quantization index modulation method (QIM) is presented. The method embeds information by modulating indices with the embedded information and then quantizing the cover media with the associated sequence of quantizers. Another common technique is difference expansion. The information hiding scheme utilizing difference expansion is presented in [9]. In this scheme side information in the form of a tracing table is produced during the information concealment process. The table is recommended to be transmitted separately from the cover image to extract a secret message. Pixel value differencing and hamming distance are used in the data hiding method for Absolute Moment Block Truncations Coding compressed images in [10]. Lastly, there are histogram shifting based schemes. The reversible information hiding technique based on reducing invalid shifting of pixels in histogram shifting is presented in [11].

Adaptive data hiding schemes aim to exploit the cover properties to achieve better results. In [12], the embedding is performed into parts of the image corresponding to edges due to the fact that humans are less sensitive to changes in those parts compared to the smooth locations. In [13], the adaptive algorithm of information unmistakable embedding into digital images is presented. This algorithm's adaptivity is in the choice of secret message bits distribution among cover coefficients which is made possible by the introduction of the "empty" value. Such adaptivity results in higher imperceptibility.

Information can take many forms and data hiding schemes are dependent on the media they are intended to be used with. For instance, in [14] steganography for printed matter that can be employed

in the anti-counterfeiting for product external packing in the Internet of Things (IoT) is discussed, in [15] the secret message is embedded into the cover of a quantum channel in steganography protocol for Fog Cloud IoT and in [16] the noise resilient audio steganography technique is proposed to be used in IoT networks.

The following works deal with digital image steganography. In [17], the EGC protocol aimed at securing data in IoT is introduced. It employs both cryptography and image steganography techniques. For steganography, the Matrix XOR encoding is implemented. In [18], the S-CycleGAN approach that embeds a secret message in the process of image-to-image translation is presented. The security is improved via the steganalysis module and the technique is adapted to secure IoT communications. In [19], the approach based on the generative adversarial networks is demonstrated. Instead of embedding secret data into original cover images, the scheme hides them in the generated foreground object region of the generated images.

Moreover, data hiding methods seem to present special interest in the IoT-healthcare field. In [20], the data securing model for IoT-based healthcare systems that exploits hybrid embedding and steganography in the DWT domain is proposed. Steganography, among other things, serves to remove the suspicion in having concealed information. In [21], the method for the secure embedding of electronic patient records into medical images is demonstrated. It uses optimal pixel repetition and pixel permutation to hide data in an imperceptible way and achieve high embedding capacity. Another scheme to be used in the Internet of Medical Things is proposed in [11].

The listed studies provide important insights into the field of information concealment as well as enable to indicate the ideas that could be applied in the improved steganographic scheme.

3. Proposed Method

In the proposed scheme information hiding is performed into the digital images' frequency domain. Multiple methods can be used to transfer an image from spatial to frequency domain and back. In this work, the Integer Wavelet Transform (IWT) is chosen due to its ease of use. It is a variation of DWT which differs by the use of integer coefficients instead of real ones. That helps to significantly lower the number of errors in an extracted secret message introduced by the use of an information hiding algorithm, hence maintaining communications at a more dependable level. IWT groups frequency coefficients into four groups that are approximate, horizontal, vertical, and diagonal coefficients denoted as cA, cH, cV and cD.

The process of information embedding can be either scalar or block. In scalar embedding, one bit of secret message is embedded into one image pixel or coefficient. On the other hand, in block embedding, more than one pixel or coefficient is used as one embedding element in which one bit is placed. Both are used in the current work. The symbol k denotes the number of frequency coefficients that are taken as one embedding element. Its value depends on the bit per pixel (bpp) value: $bpp = \frac{n}{H \cdot W}$, where n is the message length; H, W are height and width of the image in pixels. The number of frequency coefficients in one embedding element k can be found as (1):

$$k = \begin{cases} 1, & bpp > 0.5 \\ 2, & 0.5 \geq bpp > 0.25 \\ 4, & 0.25 \geq bpp > 0.125 \\ 8, & otherwise \end{cases}, \quad (1)$$

when $k = 1$ the embedding is scalar otherwise it is block. In the first case coefficients are changed to correspond to the message bits. In the second case coefficients in the block are changed in such a way that a block function corresponds to the given message bits. The function that relates block coefficients

$e_1, e_2 \ldots e_k$ with one scalar value x is required for the second case. The following function (2) is chosen due to the minimal changes in $e_1, e_2 \ldots e_k$ that could lead to the change of x.

$$x = \sum_{i=1}^{k} e_i. \tag{2}$$

The algorithm makes use of the Chinese remainder theorem (CRT). According to it if $a_1, a_2, \ldots a_n$ are pairwise coprime and $r_1, r_2, \ldots r_n$ are integers such that $0 \leq r_j < a_j$ for $j = 1, 2, \ldots n$ then there exists one and only one $x < \prod_{i=1}^{n} a_i$ such that:

$$\begin{cases} x \equiv r_1 (mod\ a_1) \\ x \equiv r_2 (mod\ a_2) \\ \quad \ldots \\ x \equiv r_n (mod\ a_n) \end{cases},$$

where "≡" denotes modular congruence.

The presented algorithm implements the adaptive embedding i.e., the dissimilarities between the image before and after the embedding process and minimized. In order to do so the binary secret message is first transformed to the ternary form though the addition of "empty" values [13] (Figure 2). Moreover, the use of empty values enables to perform embedding adaptively without a necessity to exchange additional information such as the key. Further, the empty value is denoted as −1. To optimize the time complexity of the algorithm an adaptive search is done separately for cover space fragments of a set size of 8 embedding elements. The process described is illustrated in Figure 3.

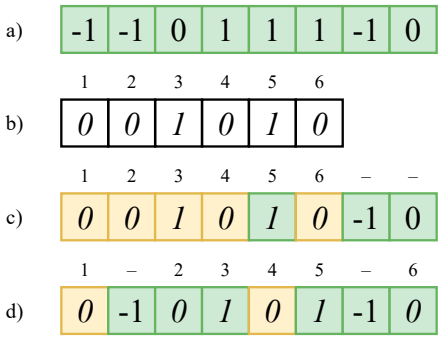

Figure 2. Example of embedding with empty values: (**a**) initial embedding fragment; (**b**) message fragment that is to be embedded in the initial embedding fragment; (**c**) first possible message distribution: 3/8 values match initial space; (**d**) second possible message distribution: 6/8 values match initial space. The second option is superior.

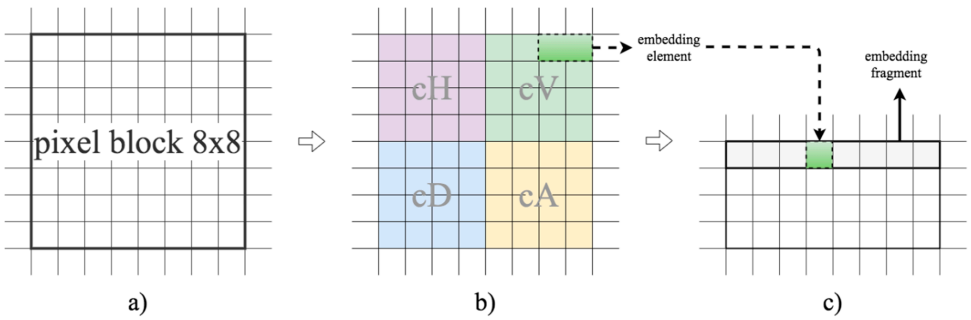

Figure 3. Embedding cover space preparation: (**a**) original image is divided into 8 × 8 pixel blocks; (**b**) IWT is applied to each block; (**c**) every set of k coefficient corresponds to one embedding element and eight embedding elements to one embedding fragment.

The novelty of the proposed scheme is combining CRT and the empty values concept to achieve good imperceptibly. The following form of CRT is used:

$$\begin{cases} x \equiv r_1 (mod\ a_1) \\ x \equiv r_2 (mod\ a_2) \end{cases}$$

The a values are chosen to minimize cover distortion as $a_1 = 2$, $a_2 = 3$. It is possible to use different values as long as they are coprime, however, higher a values lead to lower imperceptibility and increase the time complexity of the proposed scheme. The r_1, r_2 are found from a_1, a_2 and $x = \sum_{i=1}^{k} e_i$. Next, it is possible to link r_1, r_2 to the ternary embedded message value m using the following logic (3):

$$m = \begin{cases} -1,\ if\ r_1 (mod\ 2) + r_2 (mod\ 2) = 2 \\ r_1 (mod\ 2) + r_2 (mod\ 2),\ otherwise \end{cases} \tag{3}$$

Further the algorithm of information embedding is presented. Indexes 2 and 3 will be used to denote binary and ternary vectors, respectively.

Input:

Cover image, binary secret message M_2 of length n_2.

Output:

Image with secret message embedded.

Step 1. Determine k using n_2 and (1).

Step 2. Divide the cover image into not overlapping blocks 8×8 pixels.

Step 3. Apply IWT to each block 8×8 pixels.

Step 4. Determine the length of message fragment corresponding to each cover space fragment:

Step 4.1. Every set of k coefficients results in one embedding element x (2). The resulting length of the embedding space is $s = W{\cdot}H/k$ where W, H are width and height of the cover image.

Step 4.2. One fragment contains 8 elements. The number of fragments is $f = s/8$.

Step 4.3. The secret message is divided regularly among embedding fragments. For each fragment there are vector b_2 of length n_2/f from M_2 and vector b_3 of length 8 from the ternary message M_3.

Step 5. Using the extraction algorithm get the ternary message M_3 of length n_3 from the cover image ($n_2 \leq n_3$). M_3 will contain 0, 1 and empty values that are denoted as -1.

Step 6. For each fragment all possible distributions of b_2 among b_3 are considered (Figure 2). The b' is b_2 with empty values added such that the Hamming distance between b' and b_3 is minimal.

Step 7. In each fragment the determined b' message fragment is embedded.

Step 7.1. Using CRT, condition (3) and fixed a_1, a_2 the m is determined.

Step 7.2. The x is incremented or decremented resulting in x' until $m = m'$ where m' is a value from b' corresponding to the current fragment. The final change in x is $c = x' - x$.

Step 7.3. The number c is pseudo-randomly distributed among k coefficients. The x changes to x' and the corresponding value from m to m'.

Step 8. Apply inverse IWT to each block 8×8 pixels.

Step 9. Join blocks. The final image contains secret message.

The information extraction algorithm is presented below.

Input:

Image with secret message embedded, length of secret message n_2.

Output:

Binary secret message M_2.

Step 1. Determine k using n_2 and (1).

Step 2. Divide the cover image into not crossed blocks 8×8 pixels.

Step 3. Apply IWT to each block 8×8 pixels.

Step 4. Determine the number of message bits per fragment as $\frac{8 \cdot k \cdot n_2}{W \cdot H}$.

Step 5. Iterate through all fragments and extract a corresponding number of message bits missing empty values.

Step 5.1. Using CRT, condition (3) and fixed a_1, a_2 the m is determined. Append this value to the vector M_2 or set $M_2 = m$ if it does not exist yet.

For illustration purposes, a flowchart demonstrating shortened embedding and extraction processes is given in Figure 4. To look more closely on the embedding process, given one element consisting, for example, of frequency coefficients $e_1 = 132$, $e_2 = 0$, $e_3 = -14$, $e_4 = 5$ (in this case $k = 4$, thus there are four coefficients) those coefficients are connected to one scalar value x with accordance to (2) as $x = 131 + 0 + (-16) + 5 = 123$. Using x and $a_1 = 2$, $a_2 = 3$ the r_1 and r_2 are determined as $r_1 = 123 \ mod \ 2 = 1$, $r_2 = 123 \ mod \ 3 = 0$. The m is determined in accordance with (3) as $m = 1(mod\ 2) + 0(mod\ 2) = 1$. The m is compared against the intended value m' and because they differ the x' (initially $x' = x$) is decremented or incremented by 1 until $m = m'$. After a few tries the $x' = 120$ is found ($r_1 = 120 \ mod \ 2 = 0$, $r_2 = 120 \ mod \ 3 = 0$, $m = 0(mod\ 2) + 0(mod\ 2) = 0$). The difference $c = x' - x = -3$ is calculated and the initial frequency coefficients are modified so $e_1 + e_2 + e_3 + e_4 = 131 + 0 + (-16) + 5 = 120$. During extraction, frequency coefficients $\{131, 0, -16, 5\}$ are used to calculate x, then r_1, r_2 and m in the same manner as during embedding.

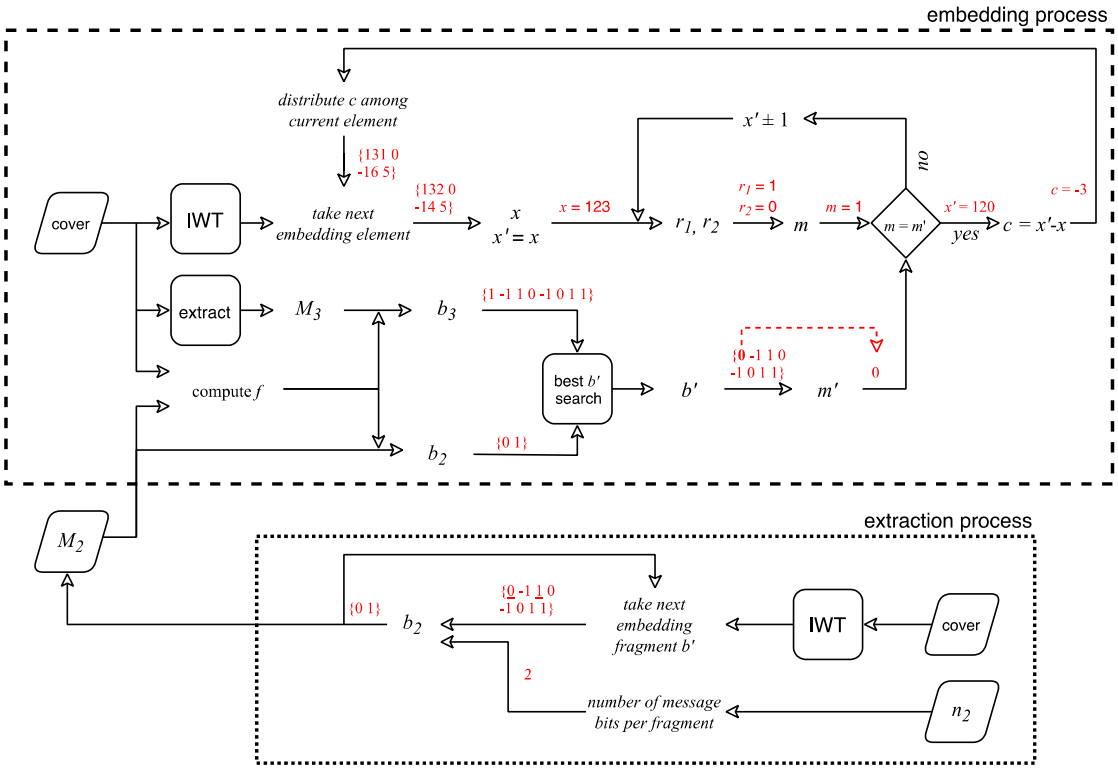

Figure 4. A flowchart demonstrating shortened embedding and extracting processes of the proposed method. The red color denotes example values.

The evaluation of the presented algorithm is located in the next section.

4. Results

4.1. Method Evaluation

The information hiding method presented in the previous section was evaluated via computing experiments and results are presented in the current section. All experiments were held in MATLAB R2020a on computer 8 GB 1600 MHz DDR3 memory and 1.8 GHz Intel Core i5 processor. The secret message is a pseudo-random stream of bits generated via MATLAB function *randi*.

The peak signal-to-noise ratio (PSNR) is used as a measure of imperceptibility. The PSNR values for different lengths of secret message are presented in Figure 5. The test was held on 20 common greyscale images 512×512 pixels [22] transformed in PNG format. The maximum possible capacity equals 262.14 kbit for test images of the aforementioned size. At such capacity, the PSNR approximately equals 44.5 dB while the least allowable PSNR is 37 dB. However, it is important to note that empty values can only occur if the embedded message is less than the maximum possible capacity. Therefore, it is recommended to use the scheme with secret messages being shorter than the upper limit. The PSNR is found as follows:

$$PNSR(I, I') = 10 \log_{10} \frac{255^2}{MSE(I,I')},$$
$$MSE(I, I') = \frac{1}{nm} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - I'(i,j)]^2$$

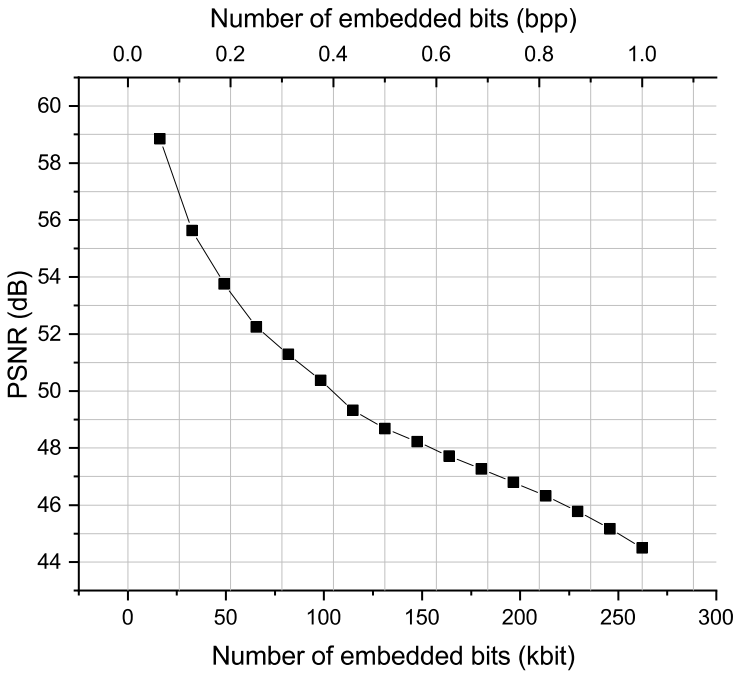

Figure 5. PSNR of the proposed method depending on the number of embedded bits for greyscale 512×512 pixels images.

Figure 6 shows a cover image and a stego image containing a secret message of maximum possible length. The differences are visually imperceptible. On Figure 7, images' histograms are presented. It can be seen that divergences are small.

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

Figure 6. Barbara.png: (**a**) before the embedding process; (**b**) after the embedding process.

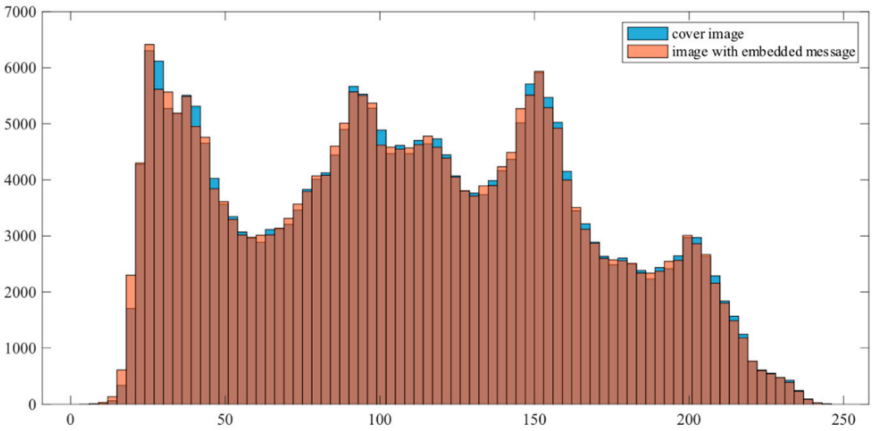

Figure 7. Barbara.png: comparison of histograms before and after embedding.

Next, the evaluation of the number of mistakes introduced by information embedding is held. The depth of test images is 8-bit meaning that pixel values range from 0 to 255. During the embedding process values in the frequency domain may change in a way that the corresponding pixels will be less than 0 or more than 255 which is called underflow and overflow problems respectively. When the message is transformed back into the spatial domain, those pixel values will be cut which can introduce some mistakes in the extraction process. The bit error rate (BER) values are used to evaluate the number of mistakes in extracted messages:

$$BER(M, M') = \frac{\sum_{i=1}^{n} M(i) \oplus M'(i)}{n}$$

where M is the original secret message, M' is the message obtained during extraction process and n is the length of M. It could be seen that the number of mistakes is small. For all test images and test message lengths, the average $BER = 1.9 \times 10^{-3}$.

Moreover, the time complexity of the proposed method is evaluated. The embedding time begins when the image and message are already read and stops after the image with a secret message is reconstructed. Mean embedding and extraction times are presented in the Table 1.

Table 1. Time complexity of the algorithm.

Message Length (kbit)	Embedding Time (Seconds)	Extraction Time (Seconds)
16.4	6.97	2.2
32.8	17.81	3.38
49.2	11.39	3.48
65.5	17.57	2.77
81.9	15.95	2.41
98.3	10.34	2.38
114.7	7.69	2.53
131.1	30.4	2.68
147.5	27.32	2.65
163.8	27.87	3.21
180.2	23.73	2.88
196.6	15.35	2.46
213.0	12	2.28
229.4	9.42	2.41
245.8	8.45	2.45
262.1	6.16	2.2
Average	15.53	2.65

As can be seen from the table the embedding time suffers some fluctuations. It is because the number of combinations $\binom{n}{k}$ that algorithm needs to undergo during adaptive embedding depends on the embedding element length k that changes with message length. The time corresponding to the maximum message length in table is time the algorithm takes without adaptative embedding.

Finally, to demonstrate the effectiveness of the adaptive embedding the comparison of number of coefficients changed with and without it is presented in Table 2.

Table 2. Number of changed coefficients.

Message Length (kbit)	Without Adaptive Embedding (%)	With Adaptive Embedding (%)
16.4	4.63	3.40
32.8	8.97	6.52
49.2	13.45	10.12
65.5	16.80	17.91
81.9	21.01	15.20
98.3	25.22	19.00
114.7	29.42	24.50
131.1	30.44	33.63
147.5	34.35	24.80
163.8	38.06	27.51
180.2	41.96	31.20
196.6	45.69	34.56
213.0	49.57	39.77
229.4	53.30	44.58
245.8	57.17	52.89
262.1	60.85	60.85
Average	33.18	**27.90**

As can be seen from Table 2, the adaptive embedding lowers the number of changed coefficients required to embed the message on average by 5%.

4.2. Comparisons with Other Data Hiding Methods

Further the presented algorithm is compared with a few other information hiding schemes. The test images are presented in Figure 8.

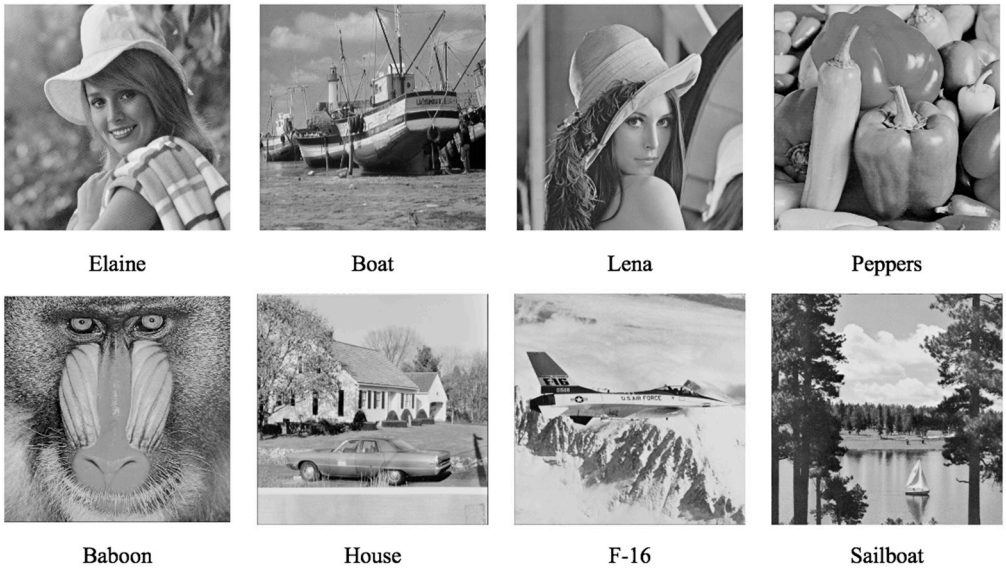

Figure 8. Some test images used in the evaluation process.

In [9], an information hiding scheme based on difference expansion is proposed. The comparison with the proposed algorithm is presented in Table 3. Contrary to our scheme the embedding capacity of [9] depends on the cover while our scheme reaches 1 bpp regardless of the image. It could also be seen that imperceptibility for given capacities is higher in our scheme, therefore our scheme outperforms [9] both in capacity and imperceptibility. However, the disadvantage of our scheme is a significant computational time.

Table 3. Comparison with information hiding scheme for digital images using difference expansion and modulus function [9].

Image	Embedding Capacity (bpp)	PSNR [9] (dB)	PSNR Proposed (dB)	Computational Time [9] (Seconds)	Computational Time Proposed (Seconds)
Elaine	0.0673	56.2007	58.034	3.738	7.1448
Boat	0.0658	56.1899	58.77	3.122	4.9716
Lena	0.0958	54.5336	56.871	3.721	6.277
Peppers	0.0807	55.1808	57.82	3.622	7.4901
Baboon	0.0389	58.2953	60.972	3.726	6.6042
House	0.1181	54.593	55.157	3.656	5.0032
F-16	0.1378	53.478	55.193	3.839	7.8503
Sailboat	0.0684	56.0315	58.583	3.718	8.181
Average	0.084	55.563	**57.675**	**3.643**	6.690

The comparison with data hiding schemes in [7,23] is presented in Table 4. As can be seen, the PSNR values for the proposed algorithm are significantly higher than [23] indicating an improvement in imperceptibility. The proposed algorithm also slightly outperforms [7] in imperceptibility measured both in PSNR and SSIM and has a higher maximum capacity that is 1 bpp against 0.75 bpp. However, our scheme lacks [7,23] reversibility quality.

Table 4. Comparison with a new high capacity and reversible data hiding technique [7] and encrypted signal-based reversible data hiding with public key cryptosystem [23].

Image	PSNR 0.25 bpp (dB)		PSNR 0.5 bpp (dB)		PSNR 0.75 bpp (dB)		SSIM 0.75 bpp	
	[23]	Proposed	[23]	Proposed	[7]	Proposed	[7]	Proposed
Lena	42.85	52.284	39.83	48.713	46.3661	46.72	0.9869	0.9889
F-16	42.84	52.021	39.84	48.33	46.3658	46.42	0.9869	0.9874
Peppers	42.85	52.356	39.83	48.814	46.3670	46.958	0.9868	0.9907
Sailboat	42.87	52.335	39.85	48.926	–	–	–	–
Boat	42.81	52.367	39.81	48.888	46.3725	47.017	0.9894	0.9930
Baboon	42.85	52.499	39.84	49.142	46.3707	47.268	0.9932	0.9964
Average	42.85	**52.310**	39.83	**48.802**	46.3684	**46.88**	0.9886	**0.9913**

The comparisons that are presented in Tables 3 and 4 are partly visualized in Figures 9–11.

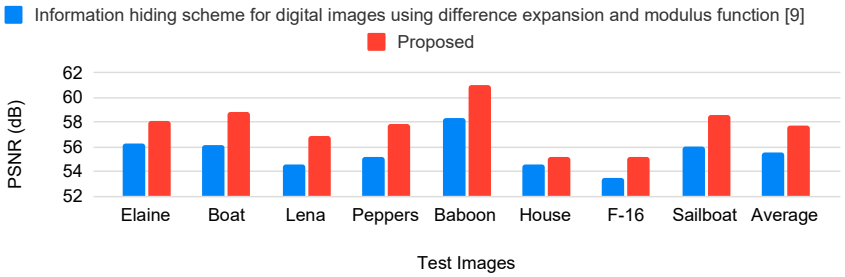

Figure 9. Comparison with information hiding scheme for digital images using difference expansion and modulus function [9].

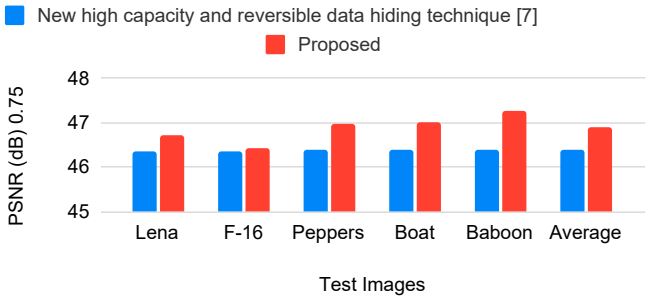

Figure 10. Comparison with A new high capacity and reversible data hiding technique [7].

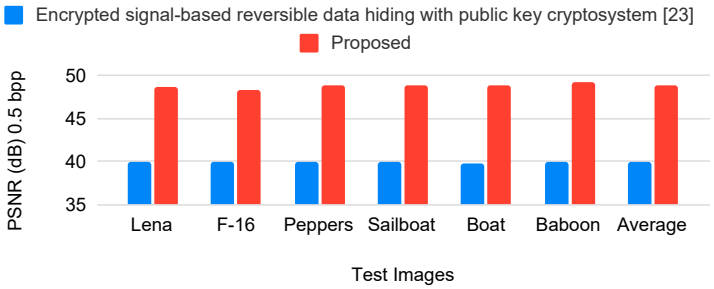

Figure 11. Comparison with encrypted signal-based reversible data hiding with public key cryptosystem [23].

The results presented in this section indicate that the proposed algorithm has good performance and can compare with other information hiding schemes.

5. Discussion

This work presents a novel adaptive information embedding scheme based on the Chinese remainder theorem. Experiments to evaluate the scheme were held in MATLAB and results are presented in the current work. The scheme is shown to achieve imperceptibility and capacity as high as 44.5 dB for secret messages of 1 bpp. The example image before and after the embedding process is provided along with histograms. Images as well as histograms do not seem to differ in any significant way. Good imperceptibility qualities are achieved through adaptive embedding that lowers the number of changed coefficients by 5%. The number of mistaken extracted bits caused by the proposed embedding scheme is evaluated using BER and on average it equals 1.9×10^{-3}. This number is tolerable. Moreover, the advantage of the presented scheme is the ability to not exchange any additional information by setting the secret message size constant. The comparisons with other information embedding techniques indicate relatively good imperceptibility and capacity qualities of the proposed scheme.

One important limitation of the proposed scheme is high time complexity. However, the method is asymmetric, with embedding time being larger than the extraction time. Thus, it is proposed to process embedding on high-performance servers while extraction can occur at end devices.

The data hiding scheme could be used in various applications involving data transfers. One relevant area where research on security is rapidly evolving is IoT. Multiple data hiding schemes to be used in IoT have already been proposed. The differences of the proposed scheme and other data security with data hiding schemes are presented in Table 5.

Table 5. Differences evaluation of the proposed scheme with other data security through data hiding schemes.

Data Security Technique	Cover Media	Application	Difference with the Proposed Method
Fractional-order spatial steganography [14]	Printed matter	Anti-counterfeiting for product external packing	Cover media
Secure quantum steganography protocol [15]	Quantum channel	Fog cloud	Cover media
Lightweight noise resilient steganography scheme [16]	Audio	Securing communications	Cover media
EGC protocol [17]	Digital image/video	Healthcare/protection against data infiltration during transmission over the IoT network	Protocol implementing both cryptography and steganography while the proposed method is focused only on data hiding
S-Cycle GAN [18]	Digital image	Covert communications	Cover images are generated while in the proposed method data is hidden in the given images
Image Steganography Based on Foreground Object Generation by Generative Adversarial Networks [19]	Digital image	Mobile edge computing	Cover images are generated while in the proposed method data is hidden in the given images
Secure medical data transmission model [20]	Digital image	Healthcare	The scheme is tested on significantly lower capacities than the proposed method
Reversible data hiding exploiting Huffman encoding with dual images [11]	Digital image	Healthcare	Dual stego images and key are used for extraction while in the proposed method one image suffices
A reversible and secure patient information hiding system [21]	Digital image	Healthcare	The closest to ours; not enough data to compare imperceptibility at the same capacity and time complexity with the proposed method

Overall, the analysis of applications of embedding methods indicates that they could be divided into two big groups. Further subgrouping depends on the particular task. The aforementioned two groups are:

(1). Both embedding and extraction algorithms are lightweight and could be processed on server and end device. There could be a hidden transmission of end device's data (sensors reading, end device state and actions, etc.) towards the server and transmission of data and commands that are needed to control the end device from the server towards the end device.

(2). The embedding algorithm is computationally complex while an extraction algorithm is lightweight. In that case, it is challenging to perform the embedding on end devices with low power consumption. Thus, it is better to have a simplex channel between the server and the end device. However, it is still possible to organize a feedback channel if the embedding is performed not on a low-powered device but on a significantly more powerful mobile device that is used as a gateway.

The proposed method belongs to the second group. Its potential applications are presented in Figure 12.

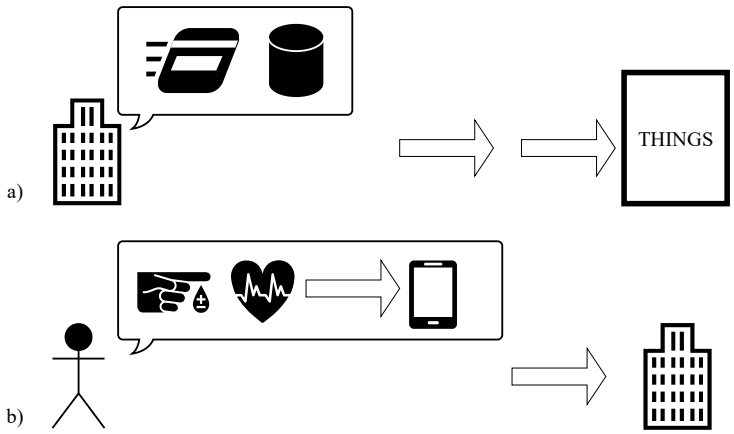

Figure 12. The proposed algorithm applications (**a**) server transfers confidential data towards end devices without intermediate devices; (**b**) wearable Internet of Things.

In the first application, a server transfers confidential data towards an end device without intermediate devices. The second application is a more interesting case and appropriate for the Wearable Internet of Things (WIoT). In this case, a person wears some number of low-powered IoT devices (such as glucose monitors, pacemakers) and a more powerful mobile device (such as a mobile phone, a tablet, a notebook) that serves as a gateway. Wearable devices produce data and send them to a gateway. The gateway embeds data into images (e.g., taken with a camera) and sends images to the server. The proposed algorithm's characteristics makes it suitable for the former application.

6. Conclusions

In the modern world ways of securing data should satisfy the requirements presented by the rapid technological development. Data hiding methods are capable of improving system security, especially when used among other data protection techniques. The main contribution of this work is presenting a novel data-hiding algorithm. The algorithm employs the Chinese remainder theorem and ternary logic. It embeds secret data into the digital image frequency domain. The most prominent feature of the proposed algorithm is outstanding imperceptibility achieved through the use of adaptive embedding. The algorithm can be used along with cryptography to ensure data confidentiality. Future research could focus on improving the time complexity of the proposed algorithm to make it more lightweight.

Author Contributions: Conceptualization, O.E.; methodology, O.E. and K.D.; software, K.D.; validation, O.E. and K.D.; formal analysis, O.E. and K.D.; investigation, K.D.; resources, O.E.; data curation, O.E.; writing—original draft preparation, O.E. and K.D.; writing—review and editing, O.E. and K.D.; visualization, K.D.; supervision, O.E.; project administration, O.E.; funding acquisition, O.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Russian Science Foundation, grant number 19-71-00106.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Amin, F.; Ahmad, A.; Choi, G.S. Towards trust and friendliness approaches in the social Internet of Things. *Appl. Sci.* **2019**, *9*, 166. [CrossRef]
2. Kadhim, I.J.; Premaratne, P.; Vial, P.J.; Halloran, B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing* **2019**, *335*, 299–326. [CrossRef]
3. Simmons, G.J. The prisoners' problem and the subliminal channel. In *Advances in Cryptology*; Springer: Boston, MA, USA, 1984; pp. 51–67.

4. Anderson, R.J.; Petitcolas, F.A. On the limits of steganography. *IEEE J. Selected Areas Commun.* **1998**, *16*, 474–481. [CrossRef]
5. Johnson, N.F.; Jajodia, S. Exploring steganography: Seeing the unseen. *Computer* **1998**, *31*, 26–34. [CrossRef]
6. Devi, S.; Sahoo, M.N.; Muhammad, K.; Ding, W.; Bakshi, S. Hiding medical information in brain MR images without affecting accuracy of classifying pathological brain. *Future Gener. Comput. Syst.* **2019**, *99*, 235–246. [CrossRef]
7. Parah, S.A.; Ahad, F.; Sheikh, J.A.; Bhat, G.M. Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. *J. Biomed. Inform.* **2017**, *66*, 214–230. [CrossRef] [PubMed]
8. Chen, B.; Wornell, G.W. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. Inf. Theory* **2001**, *47*, 1423–1443. [CrossRef]
9. Maniriho, P.; Ahmad, T. Information hiding scheme for digital images using difference expansion and modulus function. *J. King Saud Univ.-Comput. Inf. Sci.* **2019**, *31*, 335–347. [CrossRef]
10. Kumar, R.; Kim, D.-S.; Jung, K.-H. Enhanced AMBTC based data hiding method using hamming distance and pixel value differencing. *J. Inf. Secur. Appl.* **2019**, *47*, 94–103. [CrossRef]
11. Gull, S.; Parah, S.A.; Muhammad, K. Reversible data hiding exploiting huffman encoding with dual images for IoMT based healthcare. *Comput. Commun.* **2020**, *163*, 134–149. [CrossRef]
12. Kumar, S.; Singh, A.; Kumar, M. Information hiding with adaptive steganography based on novel fuzzy edge identification. *Def. Technol.* **2019**, *15*, 162–169. [CrossRef]
13. Evsutin, O.; Kokurina, A.; Meshcheryakov, R.; Shumskaya, O. The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation. *Multimed. Tools Appl.* **2018**, *77*, 28567–28599. [CrossRef]
14. Pu, Y.-F.; Zhang, N.; Wang, H. Fractional-Order Spatial Steganography and Blind Steganalysis for Printed Matter: Anti-Counterfeiting for Product External Packing in Internet-of-Things. *IEEE Internet Things J.* **2018**, *6*, 6368–6383. [CrossRef]
15. Abd El-Latif, A.A.; Abd-El-Atty, B.; Hossain, M.S.; Elmougy, S.; Ghoneim, A. Secure quantum steganography protocol for fog cloud Internet of Things. *IEEE Access* **2018**, *6*, 10332–10340. [CrossRef]
16. Djebbar, F.; Abu-Ali, N. Lightweight noise resilient steganography scheme for Internet of Things. In Proceedings of the 2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
17. Khari, M.; Garg, A.K.; Gandomi, A.H.; Gupta, R.; Patan, R.; Balusamy, B. Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *50*, 73–80. [CrossRef]
18. Meng, R.; Cui, Q.; Zhou, Z.; Fu, Z.; Sun, X. A Steganography Algorithm Based on CycleGAN for Covert Communication in the Internet of Things. *IEEE Access* **2019**, *7*, 90574–90584. [CrossRef]
19. Cui, Q.; Zhou, Z.; Fu, Z.; Meng, R.; Sun, X.; Wu, Q.J. Image steganography based on foreground object generation by generative adversarial networks in mobile edge computing with Internet of Things. *IEEE Access* **2019**, *7*, 90815–90824. [CrossRef]
20. Elhoseny, M.; Ramírez-González, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access* **2018**, *6*, 20596–20608. [CrossRef]
21. Kaw, J.A.; Loan, N.A.; Parah, S.A.; Muhammad, K.; Sheikh, J.A.; Bhat, G.M. A reversible and secure patient information hiding system for IoT driven e-health. *Int. J. Inf. Manag.* **2019**, *45*, 262–275. [CrossRef]
22. Weber, A. The USC-SIPI Image Database. Signal and Image Processing Institute of the University of Southern California. 1997. Available online: http://sipi.usc.edu/services/database (accessed on 6 December 2020).
23. Chen, Y.-C.; Shiu, C.-W.; Horng, G. Encrypted signal-based reversible data hiding with public key cryptosystem. *J. Vis. Commun. Image Represent.* **2014**, *25*, 1164–1170. [CrossRef]