applied sciences

MDPI

Article

A Content Hiding Method for Digital Hologram Using Multiple Fresnel Diffraction

Young-Ho Seo [1,†,‡], Yoon-Hyuk Lee [2,‡] and Dong-Wook Kim [1,*]

[1] Department of Electronic Materials Engeering, Kwangwoon University, Seoul 01897, Korea; yhseo@kw.ac.kr
[2] Vision System Team, Power Logics Inc., Cheongjy-si 28121, Korea; yhlee@powerlogics.kr
[*] Correspondence: dwkim@kw.ac.kr; Tel.: +82-2-940-5167
[†] Current address: 602 Chambit Hall, Kwangwoon-ro 20, Nowon-gu, Seoul 01897, Korea.
[‡] These authors contributed equally to this work.

Received: 30 June 2020; Accepted: 14 July 2020; Published: 16 July 2020

Abstract: A digital hologram (DH) is so highly valued that it needs to be protected from exposure to an unpermitted person, which could be done by a content encryption. We propose an encryption scheme for digital holograms, whose goal is to hide their information with maximal visual distortion and minimal ration of the encrypted data. It uses the characteristics of the Fresnel transform and signal processing techniques. As the diffraction distance increases the region containing the object information relative to the whole diffraction plane becomes smaller. Therefore our scheme diffracts a given digital hologram twice: the first transform for reconstructing the image contained by the hologram and the second transform for concentrating the energy of the object into a small region. Then only the energy-concentrated region is encrypted to reduce the amount of data to be encrypted. Experimental results show that when the diffraction distance of the second transform is about 20 m, the encryption ratio is only 0.0058% of the hologram data, which is enough to hide the object information unrecognizably.

Keywords: content encryption; digital hologram; Fresnel diffraction; computer generated hologram

1. Introduction

A hologram is a collection of fringe patterns generated by interference between a reference light wave and an object light wave, in which the 3-dimensional object information is stored as differential phase or amplitude from that of the reference wave [1]. Its digital content (digital hologram, DH) can be obtained by acquiring the fringe patterns with digital equipment, such as a CCD camera, or by calculating them by modeling the interference phenomenon which is called a computer-generated hologram (CGH) [2]. Because even a CGH needs a lot of time for calculations, some proposed a faster hardware implementation of a CGH method [3]. A hologram, either analog or digital, obtained either optically or by calculation, is very highly valued because its generation cost is very high and the information it contains is also very intensive [4]. Thus, there is high demanded to protect the ownership and defend against exposure to a person who is not allowed.

The usual method to protect the ownership is digital watermarking [5–8]. Some transformed the watermark data into a Fourier hologram [5] and some others used the Fresnel transform for watermark data [6] to embed it into the host DH. In another work, the watermark data were transformed to a phase-shift CGH and the result was phase-encoded [7]. In [8] various frequency transforms for 2-dimensional images were applied to the host hologram to embed a real watermark data.

To hide the DH content itself from exposing its information to the public, a content encryption method is used and there have been many studies on it. However, here only a few representative ones [9–13] are mentioned. Some proposed methods to encrypt during hologram acquisition.

Javidi et al. [9] encrypted the host DH by synthesizing the object beam without reflecting from the object and by phase retarding and random phase masking the reference beam in the interfering process. Its encryption key would be the degree of phase retarding and the random phase mask. Kim et al. [10] also used a random phase mask to distort the host DH and the result was Fresnel diffracted for encryption. The secret keys to this method are the random mask key, the diffraction distance, and the wavelength. In [11] a DH was segmented and each segment was encrypted separately by applying extended fractional Fourier transform twice, each of which had phase modification by subtraction and used three parameters. The two sets of parameters were the encryption keys for the corresponding DH segments.

The above three works encrypted the whole DH to hide all the information, but some encrypted a part of the data for the same purpose. Seo et al. [12] proposed a scheme to encrypt in the hologram domain and DCT (discrete cosine transform) and DWT (discrete wavelet transform) transform domain by calculating energy. In the hologram domain, only the two highest bit-planes of a DH were encrypted. In the DWT domain some combination of subbands were encrypted, while in the DCT domain only the DC coefficient(s) was encrypted. Among the three, the one in the DCT domain was the best and it insisted that encrypting only 0.0061% of the DH data (the entire DH was used as the unit of DCT) could hide more than 95% of the total energy. However, for some holograms, the reconstructed image after encryption shows some outlines, although they are quite dim. Seo et al. [13] also used a DWT domain named the DWPT (discrete wavelet packet transform) domain. It is a version of DWT for a subband that includes calculating the energy included. It showed that hiding only 30% of energy was enough to hide all of the information, which was 0.032% of the total hologram data.

Our method encrypts a part of DH data to hide all of the information that the DH contains. It can work with any kind of DH, no matter how it is acquired, optically or numerically. It uses the characteristic of Fresnel diffraction that as the diffraction distance increases, the relative size occupying the most electromagnetic energy diffracted from the diffraction plane becomes smaller. Thus, by adjusting the diffraction distance, only the energy-concentrated region, which would be very small part, is encrypted. Here we analyze the optimal sizes to be encrypted for various diffraction distances, the results of which are used in the experiments.

This paper consists of five sections. In the Section 2 we introduce some characteristics of the Fresnel diffraction. The proposed encryption scheme is explained in the Section 3 and the experimental results are described in the Section 4. We conclude and discuss our scheme in the Section 5.

2. Characteristics of Fresnel Diffraction

2.1. Numerical Calculation

Fresnel's transform (or diffraction) is a mathematical equation that models the diffraction phenomenon of the electromagnetic wave from a point light source, which is as Equation (1) [14].

$$g(x,y,z) = \frac{\exp^{jkz}}{j\lambda z}\int_{-\infty}^{\infty} E(u,v,0)\exp^{j\frac{k}{2\pi}\{(x-u)^2+(y-v)^2\}}\,dudv \quad (1)$$

where $E(u,v,0)$ is the complex amplitude of the electromagnetic wave from a point light source at (u,v) on the source plane at $z=0$, $g(x,y,z)$ is the complex amplitude of the electromagnetic wave at (x,y,z) resulting from diffraction, and $k=2\pi/\lambda$ is wave number for wavelength λ. If we make the discrete version of Equation (1), u, v, x, and y are discretized to $u'\Delta u$, $v'\Delta v$, $x'\Delta x$, and $y'\Delta y$ where u' or $x' \in 0,1,\ldots,M-1$ and v' or $y' \in 0,1,...,N-1$, and $M \times N$ is the resolution of the object points and the diffraction plane (here we assume that both planes have the same resolution, without losing any generality). $\Delta u \times \Delta v$ and $\Delta x \times \Delta y$ are the sampling distances on the source plane and the diffraction plane with the distance z from the source plane. The pixels in the source and the diffractions plane have the relationship of Equation (2).

$$\Delta x = \frac{\lambda z}{M\Delta u}, \Delta y = \frac{\lambda z}{N\Delta v} \tag{2}$$

Thus, Equation (2) can be rewritten with a Fourier transform as Equation (3), where $FT[x]$ means the Fourier transform of x.

$$g(x,y,z) = \exp^{j\frac{\pi}{\lambda z}\{(x'\triangle x)^2+(y'\triangle y)^2\}} FT\left[E(u,v,0)\exp^{j\frac{\pi}{\lambda z}\{(u'\triangle u)^2+(v'\triangle v)^2\}}\right] \tag{3}$$

Equation (3) may be described as the light diffracting at a point P on the input plane (the hologram plane or the spatial light modulator (SLM)) and reaching the output plane (the diffraction plane), which is shown in Figure 1.

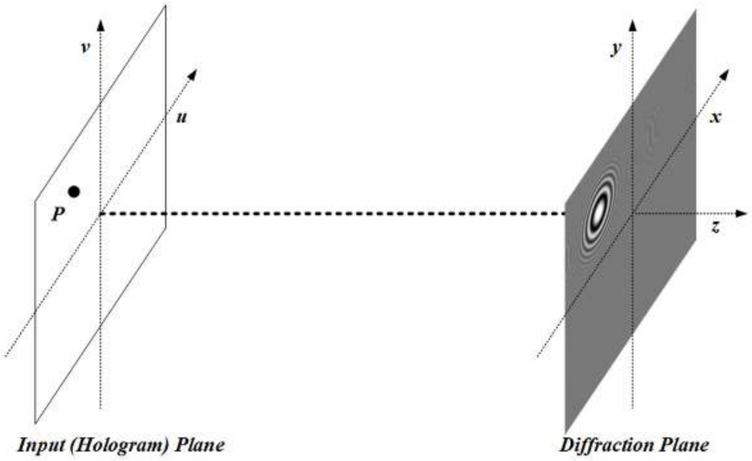


Figure 1. Diffraction between two planes.

2.2. Characteristics

The image information in a DH is reconstructed by special equipment such as a SLM. At this time the light used for reconstruction is the same as the reference light used in acquiring or generating the DH. Then the 3-dimensional object image would be formed in the space at the same distance from the SLM as that of the original object from the DH. However, for some special purpose or simulation the diffraction by the Fresnel transform is often used to reconstruct the object. Figure 2 shows three examples resulting from Fresnel diffraction for a DH at the diffraction distances of 70, 100, and 150 cm, where Figure 2b is the result when the diffraction distance is appropriate to the object. The shape of the object in the diffraction plane of Figure 2 can be confirmed to be almost unchanged in size, and the focus is changed as the distance increases or decreases. The spread (the defocused feature) of the diffracted wave in the diffraction plane by the input corresponding to y in Figure 2 can be adjusted by using the spatial frequency f_s for the distance.

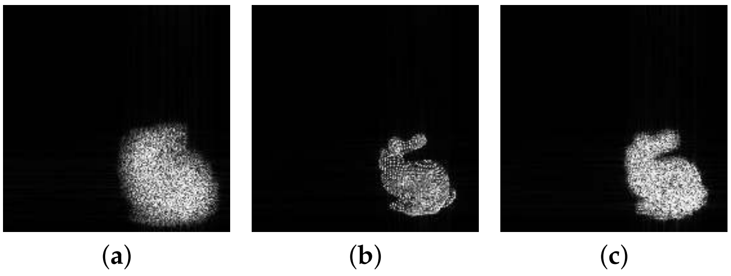
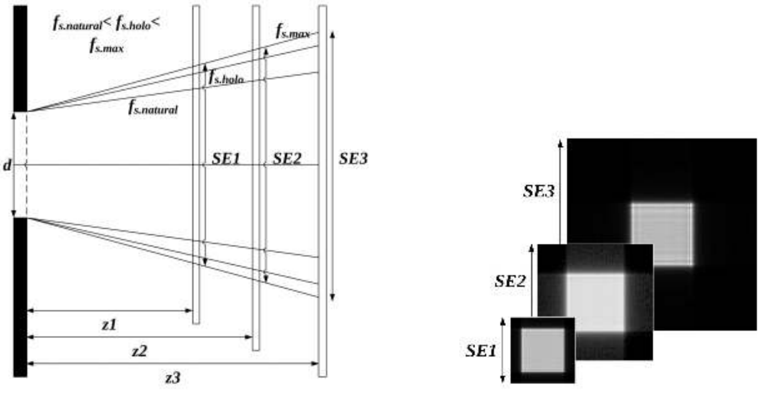


Figure 2. Result of Fresnel transform to hologram (**a**) 70 cm, (**b**) 100 cm, (**c**) 150 cm.

Figure 3 shows the spatial extension (SE) for the hologram. The SE represents the spatially extended diffraction plane with respect to the input plane. $f_{s.max}$ is the maximum frequency of the discretized hologram plane, $f_{s.holo}$ is the spatial frequency of the DH, and $f_{s.natural}$ is the frequency of the natural image. Generally, a 2D image has a lower frequency than a hologram. As the distance increases in case of a 2D image, the rate of the spread due to diffraction is smaller than that of the SE.



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

Figure 3. Spatial extent in diffraction plane according to the spatial frequency of the input plane (**a**) relationship between spatial frequency and distance (**b**) visual property.

3. Proposed Digital Hologram Encryption

A method for securing a digital hologram is a technique for encrypting content and distributing a key capable of decryption only to an authorized viewer so that a viewer without a decryption key cannot recognize the content. Since the amount of data for a still or moving DH is enormous, encrypting all of the DH requires huge computational effort.

In this paper, we propose a method to efficiently encrypt a DH. This method uses the SE property of the Fresnel transform to reduce the area to be encrypted by concentrating the energy of the restoration object into a small area.

3.1. Pre-Processing

In order to utilize the SE characteristics of the Fresnel transform at the low frequency as described in Section 2.2, the pre-processing of hologram with high frequency is required. Fresnel transform is performed for pre-processing to propagate the hologram into space. We use the Fresnel transtorm twice for two goals of diffraction and signal processing based on the SE characteristics. The first is for diffraction and the second is for signal processing.

Figure 4 shows the example result from applying the Fresnel transforms. Figure 4a shows the resulting real part and imaginary part from the first Fresnel transform, while Figure 4b shows the results by the second Fresnel transform. As we can see in the result in Figure 4b, the resultant features are scattered. That is because the results from the first Fresnel transform still contain a relatively low frequency component. To make the spatial frequency higher, a certain amount of bias is constantly added to the hologram before performing the Fresnel transform. Figure 4c shows the results from first and second Fresnel transforms after adding a bias value. The bias value converges to the center, as shown in Figure 4d. Figure 4d has higher energy than the area spread by the hologram shown in Figure 4b. By applying the signal processing technique to this area and applying the inverse transform, the modification can also be induced in the object information.

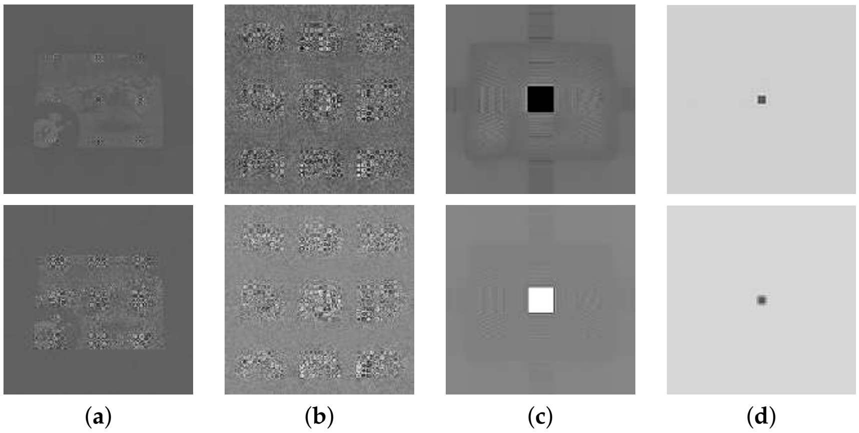


Figure 4. Fresnel transform results for holograms. Top four are real holograms and bottom ones are imaginary holograms. (**a**) Result of 1st Fresnel transform; (**b**) result of second Fresnel transform; Fresnel transform result of hologram after biasing. (**c**) Result of 1st Fresnel transform; (**d**) result of second Fresnel transform.

3.2. Content Hiding Method

Figure 5 shows the hologram encryption algorithm and an example result from each processing step, respectively. First, we add the bias value to the input hologram and perform the Fresnel transformation twice as mentioned above. The bias is experimentally obtained. Then, the concentrated area due to biasing is calculated and extracted from the result of the second Fresnel transform. The extracted data are encrypted using a kind of encryption algorithm. Then the encrypted result is replaced in its original location and the result is inverse-Fresnel-transformed twice.

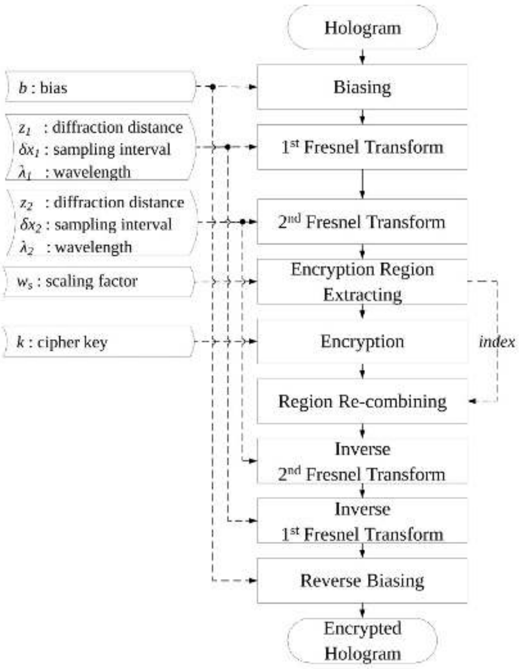


Figure 5. Hologram encryption algorithm.

In order to extract the area for encryption, the region concentrated on by the biasing is extracted from the result from the second Fresnel transform. Figure 6 shows the SEs in the Fresnel transforms to determine the concentrated area due to biasing in the second Fresnel transform. In the Fresnel transform, the SE of the diffraction plane can be expressed by Equation (4) [15], where δx is the sampling distance of the input plane.

$$SE \leq \frac{\lambda z}{\delta x} \tag{4}$$

In Figure 6, $SE1_{Max}$ and $SE2_{Max}$ are the sizes of the diffraction planes to be output and can be obtained by the input planes. $SE1_{DC}$ and $SE1_{DC}$ are the sizes of the areas encrypted by the SEs of the areas generated by the biases of the input holograms. Although the area depends on the hologram and bias value, it has a similar size to the input image because of its relatively small spatial frequency. The encryption area S_c (size of ciphering) can be calculated by Equation (5). S_c is obtained by using S_{ID} (size of input region in diffraction plane) which is the same area as the size of the input image in the second Fresnel transform and scaling parameter w_s.

$$S_c = w_s S_{ID} \tag{5}$$

$$IN1 : SE1_{Max} = S_{ID} : IN2 \tag{6}$$

$$S_{ID} = \frac{IN1IN2}{SE1_{Max}} = \frac{N\delta x_1 N\delta x_2}{\frac{\lambda_1 z_1}{\delta x_1}} = \frac{N^2 \delta x_1^2 \delta x_2}{\lambda_1 z_1} \tag{7}$$

$$R_c : N = S_c : SE2_{Max} \tag{8}$$

$$R_c = \left\lfloor \frac{NS_c}{SE2_{Max}} \right\rfloor = \left\lfloor \frac{N w_s \frac{N^2 \delta x_1^2 \delta x_2}{\lambda_1 z_1}}{\frac{\lambda_2 z_2}{\delta x_2}} \right\rfloor = w_s \left\lfloor \frac{N^3 \delta x_1^2 \delta x_2^2}{\lambda_1 \lambda_2 z_1 z_2} \right\rfloor \tag{9}$$

S_{ID} can be expressed by Equation (7) using the parameters of the first and second Fresnel transforms as the proportional expression of Equation (6). The discrete domain R_c for encryption in the result of the second Fresnel transform is expressed by Equation (9) using the proportional expression of Equation (8). N is the resolution of the input hologram plane and the output planes of the Fresnel transform. δx_1, λ_1, and z_1 are the parameters of the first Fresnel transform; and δx_2, λ_2, and z_2 are the parameters of the second Fresnel transform. Therefore, the encryption key of our scheme is the combination of the bias values, the parameter values for each Fresnel transform ($z, \delta x, \lambda$ of Equation (3)), the scale parameter for extracting the encrypted region, and the ciphering key for the cipher.

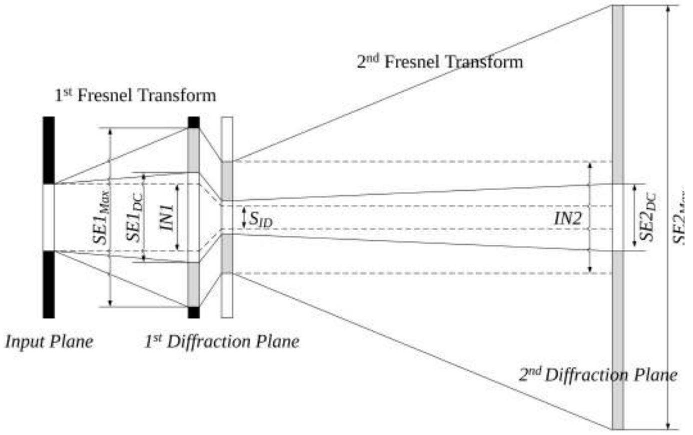


Figure 6. Diagram of the second Fresnel transform for encryption region calculation.

3.3. Recovering Method

Figure 7 shows our decryption algorithm and an example from each processing step. The decryption is performed using the encryption key combination received from the service provider. The decryption process is the same as the encrytion until the decryption step instead of encryption in the encryption process. After decrypting the encrypted area, the result replaces the extracted area.

Then the result is inverse-Fresnel-transformed—second transform first and then the first transform. Finally, the bias is removed to get the original hologram.

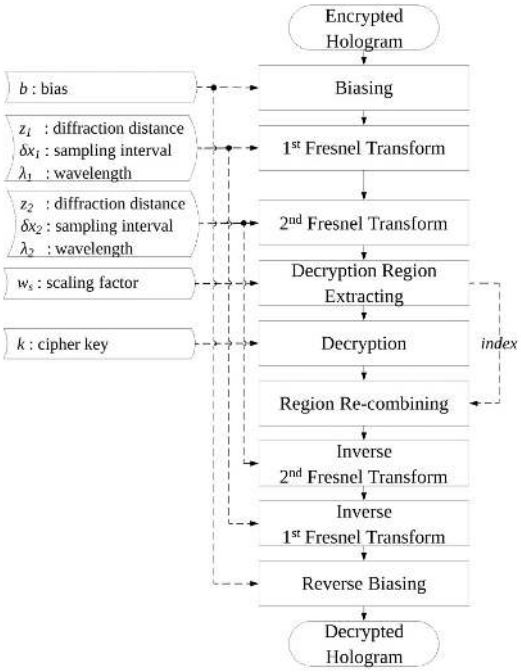


Figure 7. Hologram recovering algorithm.

4. Numerical Simulation

4.1. Experimental Environment

The proposed encryption scheme has been experimented with various digital holograms, which are generated from the images in Table 1 by a CGH method, whose parameters are listed in Table 2. For quantitative measurement, we use two quantities. The first is the NC (normal correlation) value between the image from reconstructing the original DH and the one from the encrypted DH. Both reconstructions are done by Fresnel transform at the center of the image to see how much information is hidden by encryption. The second quantity is the encryption ratio, that is, the ratio of the amount of encrypted data to that of the original data, which is as Equation (10).

$$ratio(\%) = \frac{m_c n_c}{8MN} \times 100 \tag{10}$$

Table 1. Test images for experiments.

Class	# of Images	Provided	Acquisition
1	5 including Rabbit	Depth map	Internet
2	5 including Sujin	Color+depth map	Vertical-rig system [4]
3	5 including Baby	Color+depth map	Middlebury [16]
4	5 including Billiard	Color+depth map	DOF pro [17]

In this equation, the reason why the denominator is multiplied by eight is because we encrypt only the MSB (most significant bit) for each pixel value. m_c and n_c are the width and height of the encrypted area. In order to make all holograms the same size, class 1 and 2 of Table 1 were created with a size of 1024 × 1024, and class 3 was cropped with partial holograms of 1024 × 1024 at the center.

Since the first Fresnel transform is used to generate the low frequency information, the parameters may vary depending on the object information used, as it differs each time the hologram is acquired. Therefore, only the parameters of the second Fresnel transform are shown in Table 2.

Table 2. Parameters used in the experiments for the digital hologram encryption.

Parameter		Specification
Hologram resolution		1024 × 1024
2nd Fresnel Transform	Distance (z_2)	1 m, 5 m, 20 m
	Pixel Pitch (δx_2)	10 µm
	Wavelength (λ_2)	633 nm
Scale Factor (w_s)		0.1 to 10

4.2. Experiments for the Scaling Factor and Diffraction Distance

First, we performed experiments on the scaling factor w_s in Equation (5) and the diffraction distance z_2 in Equation (9). The results are shown in Figure 8, which shows the NC values for the three diffraction distances of 1, 5, and 20 m as increasing the scaling factor to 10. In all cases, the NC values decrease to certain scaling factor values and then increase as the scaling factor increases further. The lowest NC values were obtained at the scaling factors of about 0.5, 0.7–1.3, and 2.4–4.4 and the encryption ratios were 0.094%, 0.0075–0.0252%, and 0.0053–0.0181% for the distances of 1, 5, and 20 m, respectively.

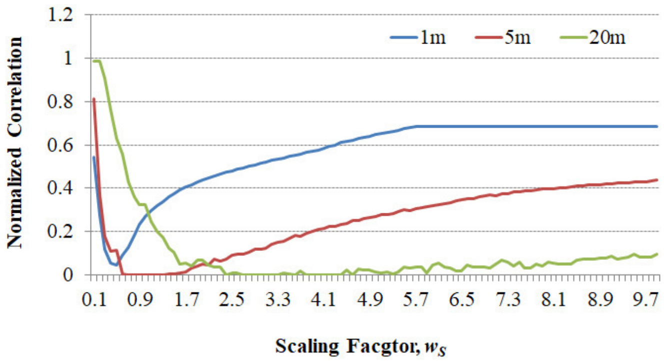


Figure 8. C (normal correlation) values according to the transform distance and scale factor of the second Fresnel transform in the proposed digital hologram encryption technique.

Figure 9 shows some example results from encrypting the Rabbit DH with the optimal scaling factors of 0.5, 0.7, and 2.4 and being reconstructed for the diffraction distances (a) 1 m, (b) 5 m, and (c) 20 m. As you can see from the figures, the size of pattern by encryption gets larger as the distance increases. In each case the information contained by the DH was completely hidden unrecognizably in the reconstructed image.

Because the encryption efficiency was better at the diffraction distance of 20 m than the other distances—Figure 8—we performed more experiments on the diffraction distance of 20 m. A few representative results for the Rabbit (class 1), Sujin (class 2), Baby (class 3), and Billiard (class 4) images are shown in Figure 10. For all the DHs, the results were almost the same as those of the lowest scaling factor value of about 2.5, giving the highest encryption effect.

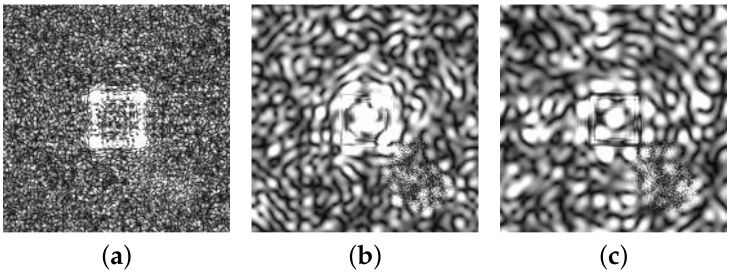


Figure 9. Examples of encryption results with the optimal scaling factor at the diffraction distances of (**a**) 1 m (s = 0.5), (**b**) 5 m (s = 0.7), (**c**) 20 m (s = 2.4).

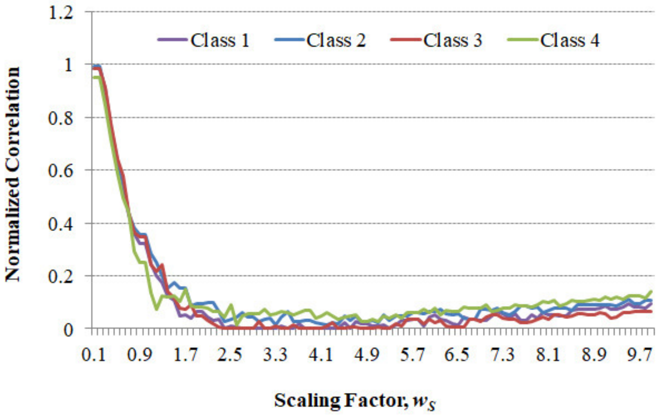


Figure 10. NC values and scale factor of the second Fresnel transform at the transform distance 20 m in the proposed digital hologram encryption technique.

For the four DHs their encrypted and reconstructed images are shown in Figure 11, for some scaling factors: (b,f,j,n) with 2.5, (c,g,k,o) with 3.5, and (d,h,l,p) with 5; and the images reconstructed without encryption (a,e,i,m). From the figures it is clear that the image gets more unrecognizable as the scaling factor increases but also it is clear that in each image the scaling factor 2.5 is enough to hide the information almost completely. The encryption ratios when the scaling factor was 2.5, 3.5, and 5 were 0.0058%, 0.0115%, and 0.0231%, respectively. Figure 12 shows the result of decrypting the encrypted hologram at a transform distance of 20 m by inputting the incorrect key and the correct key. As a result of decoding, it can be confirmed that object information is not known at all when an incorrect key is used.

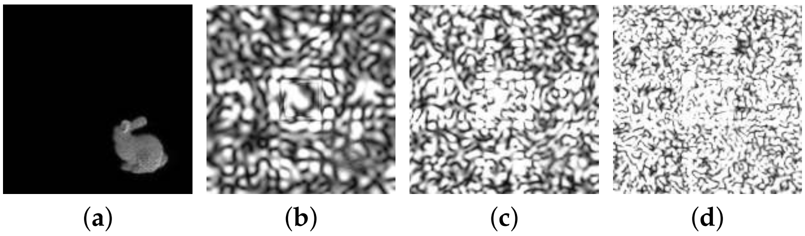


Figure 11. *Cont.*

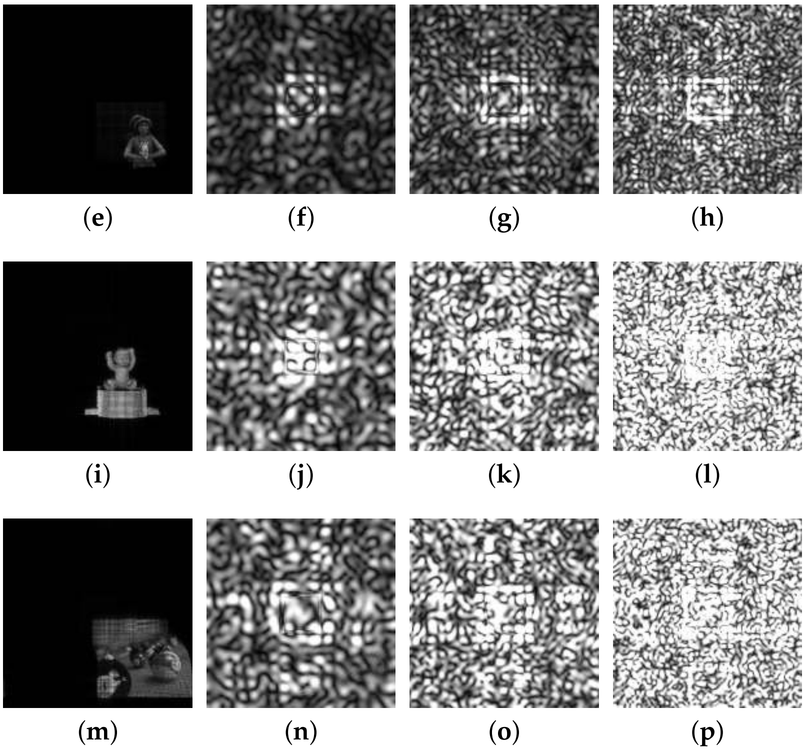


Figure 11. Examples of reconstructed images after encryption at the diffraction distance of 20 m: for the images of the Rabbit (class 1) (**a**–**d**), Sujin (class 2) (**e**–**h**), Baby (class 3) (**i**–**l**), and Billiard (class 4) (**m**–**p**); the unencrypted image (**a**,**e**,**i**,**m**); scaling factor 2.5 (**b**,**f**,**j**,**n**), 3.5 (**c**,**g**,**k**,**o**), and 5 (**d**,**h**,**l**,**p**).

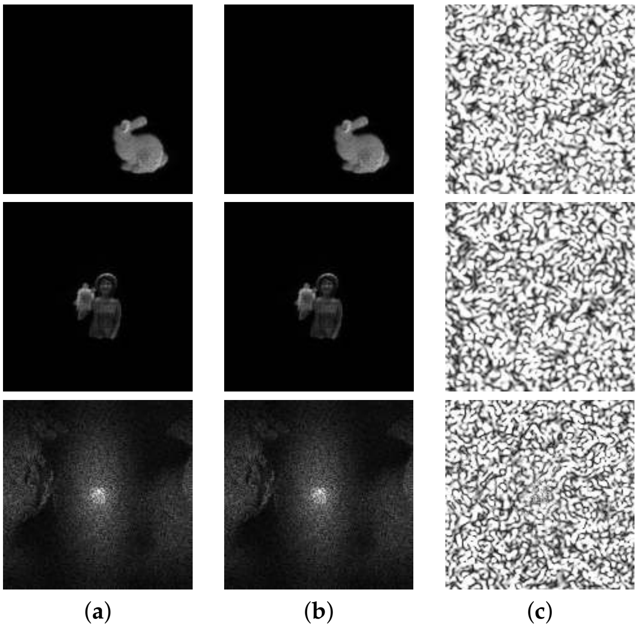


Figure 12. Examples of the reconstructed images from the decrypted hologram with (**b**) the correct key, (**c**) an incorrect key, whose original images are (**a**).

4.3. Comparison with the Previous Works

As explained in Section 1, the previous studies [9–11] encrypted a DH during the generation process such that one of the two lights for interference was changed by retardation of phase shifting, or an extra light having a special property was added. Thus, they naturally encrypted all the data in a DH so that the encrypted results hid its information completely unrecognizably. Because of the properties of light, they might suffer from decryption, but they showed good decryption results, such as 9.4 × 10^{-30} and 3.55 × 10^{-12} in MSE (mean square error) in [10,11], respectively. However, they have the inherent defect that they can only be applied during generation of a DH, not to a DH already generated.

Meanwhile, Seo et al. [12,13] used signal processing techniques like ours, such as DCT, DWT, and DWPT. Their strategies were to hide as much energy in a DH as possible by minimizing the encryption ratio. To hide more than 95% of energy, the encryption ratios were 0.0061% and 0.032% in [12,13], respectively. However, because they decided the amount of data to be encrypted on the basis of the energy in the transformed domain, some encrypted DHs revealed their information, such as contour/outlines of the object or image itself, very blurred though. However, our scheme showed only a 0.0058% encryption ratio and could hide the information in any of the tested DHs such that the object could not be recognized by close visual inspection.

Table 3 summarizes Seo's method [13] and ours for further comparisons. In the study by Seo et al. [13], the NC value was 0.65 when using 7-level DWT and a 95% energy threshold, which are the parameters used to perform most encryptions, and the encryption ratio to use 7-level DWT and 35% energy threshold was 0.032%. On the other hand, the proposed method has better NC efficiency because it has a lower NC value, though encryption is performed for a five-times smaller area than Seo's result.

Table 3. Comparison with previous research.

	The Previous Method [13]		**Proposed Method**
	$L_{TH}(7), E_{TH}(95)$	$L_{TH}(7), E_{TH}(95)$	
NC	0.65	0.8	0.0008
Encryption Ratio	-	0.032%	0.0058%

5. Conclusions

In this paper we proposed an encryption scheme for a DH to hide the information contained in the DH by encrypting as small an amount of data as possible with the maximal encryption efficiency. It is a signal processing method that uses the Fresnel transform such that the first transform is done to change the DH into the corresponding 2D object image and the second one is to concentrate the energy of the object in the image. The second transform uses the characteristic of the Fresnel transform that as the diffraction distance increases, the relative size of the object region decreases with the same resolution, which results in reducing the amount of data it is necessary to encrypt to hide all the information. In addition, we adopted a parameter called scaling factor that scales the area to be encrypted to make the encryption efficiency maximal.

Experimental results told us that only 0.0058% of the original data needs to be encrypted to hide the information unrecognizably, and it is smaller amount than any existing signal processing method. In addition, ours can apply to an already generated DH, which makes it useful for more applications than the ones that must be applied during generation of a DH. Consequently we expect that the proposed method will be used in more applications with very high encryption efficiency.

The proposed method is for the Fresnel hologram, so if it is applied to other types of holograms, it will have different results.

Author Contributions: Conceptualization, Y.-H.S. and Y.-H.L.; software, Y.-H.L.; validation, Y.-H.S. and D.-W.K.; writing-original draft preparation, Y.-H.S. and D.-W.K.; writing-review and editing, Y.-H.S.; supervision, D.-W.K.; funding acquisition, D.-W.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2019R1F1A105455212). The present Research has been conducted by the Research Grant of Kwangwoon University in 2020.

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

References

1. Benton, S.A.; Bove, J.V.M. *Holographic Imaging*; John Wiley and Sons Inc.: Hoboken, NJ, USA, 2008.
2. Reichelt, E.A. *Holographic 3-D Displays-Electro-Holography Within the Grasp of Commercialization, Advances in Lasers and Electro Optics*; INTECH: London, UK, 2010.
3. Seo, Y.-H.; Choi, H.-J.; Yoo, J-S.; Kim, D.-W. A new parallelizing algorithm and cell-based hardware architecture for high-speed generation of digital hologram. *J. Syst. Archit.* **2011**, *16*, 54–63.
4. Seo, Y.-H.; Lee, Y.-H.; Koo, J-M.; Kim, W-Y.; Yoo, J.-S.; Kim, D.-W. Digital holographic video service system for natural color scene. *Opt. Eng.* **2013**, *52*, 113106. [CrossRef]
5. Chen, C.J.; Lin, L.C.; Dai, W.T. Construction and detection of digital holographic watermarks. *Opt. Commun.* **2005**, *248*, 105–116. [CrossRef]
6. Kim, H.; Lee, Y.-H. Optimal watermarking of digital hologram of 3-d object. *Optics Express* **2005**, *13*, 2881–2886. [CrossRef] [PubMed]
7. Kishk, S.; Javidi, B. 3D object watermarking by a 3D hidden object. *Opt. Express* **2003**, *11*, 874–888. [CrossRef] [PubMed]
8. Choi, H.-J.; Seo, Y-H.; Yoo, J.-S.; Kim, D.-W. Digital watermarking technique for holography interference patterns in a transform domain. *Opt. Lasers Eng.* **2008**, *46*, 343–348. [CrossRef]
9. Tajahuerce, E.; Javidi, B. Encrypting three-dimensional information with digital holography. *Appl. Opt.* **2000**, *39*, 6595–6601. [CrossRef] [PubMed]
10. Kim, H.; Kim, D.-H.; Lee, Y.-H. Encryption of digital hologram of 3-d object by virtual optics. *Opt. Express* **2004**, *12*, 4912–4921. [CrossRef] [PubMed]
11. Wang, X.; Zhao, D. Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics. *Opt. Express* **2006**, *14*, 1476–1486. [CrossRef] [PubMed]
12. Kim, D-W.; Choi, H-J.; Choi, Y-G.; Yoo, J-S.; Seo, Y.H. Information hiding for digital holograms by electronic partial encryption methods. *Opt. Commun.* **2007**, *277*, 277–287. [CrossRef]
13. Seo, Y.-H.; Choi, H-J.; Kim, D-W. Digital hologram encryption using discrete wavelet packet transform. *Opt. Commun.* **2009**, *282*, 367–377. [CrossRef]
14. Wikipedia. Fresnel Diffraction. Available online: http://en.wikipedia.org/wiki/Fresnel_diffraction/ (accessed on 30 May 2019).
15. Kelly, D.P. Numerical calculation of the Fresnel transform. *J. Opt. Soc. Am. A* **2014**, *31*, 775–764. [CrossRef] [PubMed]
16. Middlebury. Middlebury Stereo Datasets. Available online: http://vision.middlebury.edu/stereo/data/ (accessed on 30 May 2019).
17. DOFpro. DOFpro Datasets. Available online: http://www.dofpro.com/cgigallery.htm/ (accessed on 30 July 2018).