Investigation of digital hologram watermarking with double binary phase encoding

Xiaohong Zhou*,a, Linsen Chen a, Jie Shao a
a Institute of Information Optical Engineering, Soochow University, China 215006

ABSTRACT

We propose a new method of digital watermarking with double binary optical phase encoding technique. Design procedures base on iterative Fourier transform algorithm (IFTA). The combination of two binary phase structures, in which one is used to encode the hidden image, and the other as encryption phase key, is inserted as watermark into the host image. The affections of phase levels of binary phase holograms on the quality of extracting watermark from the watermarked image have been analyzed, and results show that the 2/2 phase level combination is the best scheme of watermarking than other multiple combinations. The principle of encrypting the private key has been presented. This method can effectively increase the security of digital hologram watermarking and support the hard output of the watermarked image. The watermark is robust against hard output. We analysis the influence on the quality of extracted image after the processing of printing and scanning. We also develop the software tool for the watermarking process. The experimental results are given.

Keywords: binary optics; phase encoding; digital watermarking; diffraction.

1. INTRODUCTION

Holographic technique has been applied for digital watermarking, and the hologram watermark information cannot be removed by cutting it out of the host image. As is presented in Ref.1, the hidden image is modulated by random phase mask, and then its Fourier transformed hologram embedded into host image. The reconstructed image can be obtained by inverse Fourier transform and independently of the random phase modulation. But the hidden image can be read by unauthorized persons easily. Javidi et al. have presented an information hiding technique with double phase encoding and used it to watermarking images. It’s difficult to decode the original information without knowing the codes used in the encoding process. However, the quality of recovered image degrades heavily after printing and scanning.

In this paper we propose a new method of digital hologram watermarking with double binary optical phase encoding. Two binary phase structures are obtained by iterative Fourier transform algorithm. One is used to encode the hidden image; the other is an encryption phase key. Combination of these two structures is inserted as watermark into the host image. With this method, we analyzed the affections of phase levels of binary phase holograms on the quality of extracted image from the watermarked image (the host image containing hidden image), and results show that the 2/2 phase level combination is the best scheme of watermarking than other multiple phase step combinations. We can improve the security of watermarking and make the watermarked image robust against the hard output of watermarked image by designing key. The quality of extracted image after the processing of printing and scanning can be improved by image processing.

This paper is organized as follows. In Sec. 2, we proposed the algorithm for binary phase encoding and watermarking strategy. The principle of encrypting key is shown in Sec. 3. In Sec. 4, we evaluate the quality of reconstructed image and discuss the distortions during printing and scanning, and the experimental results verify that our method is robust against hard output. Then we give a short message about the software kit developed for encoding and decoding process of watermark. Finally, the conclusion is given in Sec. 5.

2. THE PROPOSED ALGORITHM

2.1 Binary phase encoding

*xiaozhouzh@hotmail.com; phone 0512-65112661; fax 0512-65215257
Binary phase structures are obtained by using iterative Fourier transform algorithm (IFTA) presented by Gerchberg-Saxton. IFTA has been improved by many authors. A block diagram of this algorithm is shown as Fig. 1. Let \((u,v)\) denote the object domain coordinates and \((x,y)\) denote the coordinates in image domain. The desired image, \(b(x,y)\), with an initial phase estimate \(\psi_0(x,y)\) is used to start this algorithm. The cycle is repeated until convergence is achieved. In order to get a pure phase structure, \(a(u,v)\) is replaced by constant and \(\phi(u,v)\) is quantized. The quantization rule is denoted as

\[
\phi(u,v) \in \{0, 0 + \pi/L, \ldots, \pi - \pi/L\},
\]

with \(L = 2\pi/L\). In this paper we call \(L\) phase level and prescribe: \(L=2\) denotes \(\phi(u,v) \in \{0, \pi\}\); \(L=4\) denotes \(\phi(u,v) \in \{0, \pi/2, \pi, 3\pi/2\}\); \(L=8\) denotes \(\phi(u,v) \in \{0, \pi/4, \pi/2, 3\pi/4, \pi, 5\pi/4, 3\pi/2, 7\pi/4\}\). We actually choose 20 iteration cycles, and obtain a phase structure \(\exp[i\phi(u,v)]\) whose Fraunhofer diffraction pattern can be described by \(\mathbf{FT}\{\exp[i\phi(u,v)]\}\), where \(\mathbf{FT}\) denotes the Fourier transform. The diffraction energy concentrates on \pm 1 orders and other orders can be omitted, so the diffraction wavefront field can be expressed by

\[
g_i(x,y) = g_{1i}(x,y) + g_{2i}(x,y) + n(x,y),
\]

where \(g_{1i}(x,y)\) and \(g_{2i}(x,y)\) denote the \pm 1 orders diffraction wavefront respectively, and \(n(x,y)\) describes the noise distribution on the reconstructed image due to the algorithm and quantized phase. In the case of \(L=2\), \(g_{1i}(x,y)\) and \(g_{2i}(x,y)\) are symmetrical with respect to the origin of the coordinate, we can write

\[
g_{1i}(x,y) = g_{1i}^*(x,y),
g_{2i}(x,y) = g_{2i}^*(x,y),
\]

where \(^*\) indicates the complex conjugate. When \(L=4, 8\) or more, \(g_{1i}(x,y)\) will approximate to 0 and \(g_{2i}(x,y)\) may be approximated as:

\[
g_i(x,y) = g_{2i}(x,y) + n(x,y),
\]

The diffraction efficiency of the phase structure, \(\exp[i\phi(u,v)]\), can be given by:

\[
\eta = \sum_{(x,y) \in \Omega} g_{2i}^2(x,y)/\sum_{x} \sum_{y} g_i^2(x,y).
\]

where \(\Omega\) denotes the hidden information domain, \(M\) and \(N\) are the sizes of whole image plane. According to Ref. 11, the theoretical values of \(\eta\) are 40.5%, 81% and 95% corresponding to \(L=2, 4\) and 8.

### 2.2 Watermarking strategy

The principal patterns used in the present study are shown in Fig. 2. Fig. 2(a) shows the color host image, 'lena.bmp' (256x256 pixels), whose blue channel \(C_b(u,v)\) is used to hide watermark. The hidden image \(h(x,y)\) and the designed key \(k(x,y)\) are respectively shown in Fig. 2(b) and Fig.2(c). By employing the IFTA mentioned in Sec. 2.1, we obtain phase structures, \(\exp[i\phi_1(u,v)]\) and \(\exp[i\phi_2(u,v)]\), of \(h(x,y)\) and \(k(x,y)\). (The subscript 1 and 2 will represent the related datum of hidden image and key, respectively.) The binary phase structure, \(\exp[i\phi_2(u,v)]\), is phase key and illustrated in Fig. 2(d). The reconstructed images of \(\exp[i\phi_1(u,v)]\) and \(\exp[i\phi_2(u,v)]\) can be expressed as: \(g_{1i}(x,y) = \mathbf{FT}\{\exp[i\phi_1(u,v)]\}\) and \(k_{i}(x,y) = \mathbf{FT}\{\exp[i\phi_2(u,v)]\}\). We employ the following combined phase structure,

![Figure 1: Gerchberg-Saxton algorithm.](image_url)

<table>
<thead>
<tr>
<th>Object plane ((u,v))</th>
<th>Image plane ((x,y))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(f = a \exp[i\phi])</td>
<td>(F =</td>
</tr>
<tr>
<td>Satisfy object modulus constraint (f(u,v) = a(u,v))</td>
<td>Satisfy Fourier modulus constraint (</td>
</tr>
<tr>
<td>(f =</td>
<td>f</td>
</tr>
</tbody>
</table>

Note: \(\exp[i\phi]\) is used to hide watermark. The hidden image \(C_b(u,v)\) is phase key and illustrated in Fig. 2(d).
\[
\exp[ i \Delta \phi(u, v) ] = \exp[ i \phi_1(u, v) - i \phi_2(u, v) ],
\]

as the encrypted watermark. The watermark showed in Fig. 2(e) are obtained in the case of \( L_1/L_2 = 2/2 \), where \( L_1 \) and \( L_2 \) denote phase levels of \( \exp[ i \phi_1(x, y) ] \) and \( \exp[ i \phi_2(u, v) ] \), respectively, and both can equal to 2, 4, 8 or more. The watermarking module is given in Fig. 3(a) and the watermarked image is expressed as:

\[
C(u, v) = C(u, v) + \alpha \exp[ i \phi_1(u, v) - i \phi_2(u, v) ].
\]

![Figure 2: Encoding and decoding of hologram watermarking by using the binary phase structures with phase key. (a) color host image; (b) hidden image; (c) private key; (d) binary phase structure of private key by using IFTA; (e) combined watermark; (f) watermarked image; (g) decoding with key; (h) decoding without key](image)

![Figure 3: Watermarking strategy (a) Watermarking process; (b) Watermark retrieval process](image)
where \( C_1(u,v) \) is normalization of \( C_b(u,v) \). The parameter \( \alpha \) is an arbitrary constant chosen to ensure the invisibility of the watermark and the robustness of the hidden image against distortions. In the case of \( \alpha=0.1 \), the watermarked image has a good visual quality, as seen from Fig. 2(f). It is obvious that \( C(u,v) \) is complex. During the hard output of the image file, we actually deal with the modulus of \( C(u,v) \). First step of decoding procedure is to divide the color watermarked image into three monochromatic gray scale images. Secondly, the watermarked channel \( C(u,v) \), is multiplied by phase key exp[\( i\phi_2(u,v) \)] and then transformed to Fourier domain. The watermarking retrieval process is independent of original host image and illustrated in Fig. 3(b). This process can be represented as:

\[
R(x,y) = \frac{2}{\alpha} \text{FT}(C(u,v) + \alpha \exp[ i\Delta \phi(u,v) ] \times \exp[ i\phi_2(u,v) ])
\]

where \( \text{FT} \) stands for the convolution integral. Multiplying \( \frac{2}{\alpha} \) is to make the coefficient of \( g_\eta(x,y) \) equal to 1. The first term, convolution integral of host image’s Fourier spectrum and the key image, is located in the center of reconstructed field. The second term reconstructs the hidden image \( g_\eta(x,y) \). As seen from the third term, the phase level of \( \exp[ i\phi_2(u,v) ] \) will yield the influence on quality of reconstructed image. In the case of \( L_1/L_2=2/2 \), Eq. (9) can be written as:

\[
R(x,y) = \frac{2}{\alpha} \text{FT}(C(u,v) \times g_\eta(x,y) + n(x,y)).
\]  

According to Eqs. (3) and (4), the \( \pm 1 \) orders diffraction wavefront of \( g(x,y) \) interfere with \( \mp 1 \) ones of \( g^*(x,y) \), respectively, which do not happen when \( L_1/L_2=2/2 \). In addition, based on the value of \( \eta \) given in Sec. 2.1, we know that the intensity of reconstructed image of \( L_1/L_2=2/2 \) is much higher than other combinations.

Fig. 2(g) shows the reconstructed image in the case of \( L_1/L_2=2/2 \). The intensity of the first term of Eq. (9) is much higher than the other two terms, but we can make them separated in space by rectifying the position of hidden information on the whole image. [see Fig. 2(g)].

The Fourier transform of watermarked image cannot reconstruct the hidden image, and that can be explained as:

\[
\text{FT}[C(u,v)] = \frac{2}{\alpha} \text{FT}[C(u,v)] + (\alpha \exp[ i\Delta \phi(u,v) ]) + \exp[ i\Delta \phi(u,v) ]
\]

From the second and third terms of Eq. (11), the convolution of two functions blurred the reconstructed image, as is shown in Fig. 2(h). Therefore, watermark cannot be extracted without key.

3. KEY ENCRYPTION

The Fourier spectrum of host image, \( \text{FT}[C(u,v)] \), has a strong sharp peak at center, shown in Fig. 2(h), so the convolution between \( \text{FT}[C(u,v)] \) and \( k(x,y) \) can be approximated as:

\[
\text{FT}[C(u,v)] \otimes k(x,y) = k(x,y)
\]

Eqs. (9) and (12) indicate that key image can also be reconstructed in reconstructed field. Therefore it is very necessary to encrypt key, considering security. We abide by the following rules to design the key. (1) As we can see from Fig. 2(g), the size of \( k(x,y) \) should be limited to a finite range, or the reconstructed key image and the hidden image would overlap. (2) Distribution of phase structure should change gradually in order to reduce the alignment requirement between the phase key and the watermarked image. So the hidden image can be extracted after the process of printing and scanning. (3) In the case of \( L_1=2 \), the \( \pm 1 \) orders diffraction images of phase key should be complement in position. The reconstructed image of phase key can be expressed as:

\[
k(x,y)= k_{1}(x,y) + k_{-1}(x,y)
\]

In present study, we design a key shown in Fig. 4(a). The length and width of key are 1/5 and 1/25 of the host image, respectively. Fig. 4(b) is the binary phase structure of 4(a) in the case of \( L_1=2 \). As is seen from Fig. 4(c), the diffraction image of \( k(x,y) \) is the uniform field superposed by digital noise. In this way, the spatial distribution of key cannot be known from the reconstructed field [see Fig. 4(d)]. (Fig. 4(a) and 4(c) are both enlarged by 2 times.) Any modification of pixels of \( k(x,y) \) will change the distribution of phase structure and the watermark cannot be extracted. We define the coordinates of the left upper pixel as \((1,1)\). For example, we modify the point \((124,138)\) on \( k(x,y) \), as shown by Fig. 4(e). Fig. 4(f) shows the binary phase structure of modified key in the case of \( L_1=2 \). Fig. 4(g) is the diffraction image of 4(f). We cannot extract the hidden image with the modified key, which can be illustrated by Fig. 4(h). (Fig. 4(e) and 4(g) are enlarged.) The repeated experiment is performed by modifying different pixels randomly, and the results confirm that the hidden image cannot be extracted when the key is modified more than 1%.
Figure 4: Results of original key and modified key (a) original key; (b) binary phase structure of 4(a) in the case of L2=2; (c) diffraction image of 4(c); (d) extracted image with original key; (e) modified key; (f) binary phase structure of 4(e) in the case of L2=2; (g) diffraction image of 4(f); (h) extracted image with modified key

pixels. Therefore, encrypting key improves the security of watermarking greatly.

4. DISCUSSION

4.1 Evaluation of reconstructed image

In this section, two metrics are defined to measure quality of extracted hidden image. Let \( r(x, y) \) denote the extracted hidden image from the watermarked image and \( w(x, y) \) denote diffraction image of binary phase structure obtained by IFTA. The correlation coefficient, \( C_r \), between the extracted image and the diffraction one at the target image domain (\( \Omega \)) is defined as

\[
C_r = \frac{\sum_{(x, y) \in \Omega} (A(x, y)B(x, y))/\sqrt{\sum_{(x, y) \in \Omega} A^2(x, y) \sum_{(x, y) \in \Omega} B^2(x, y))}
\]

(14)

with \( A(x, y) = w(x, y) - \mu_w(x, y) \); \( B(x, y) = r(x, y) - \mu_r(x, y) \). \( \mu_w(x, y) \) and \( \mu_r(x, y) \) are means of \( w(x, y) \) and \( r(x, y) \). The parameter \( Q \) is defined to measure the efficiency of extracting watermark. Similar to the definition of \( \eta \) [see Eq. (6)], we have

\[
Q = \sum_{(x, y) \in \Omega} r^2(x, y)/\sum_{x} \sum_{y} w^2(x, y).
\]

(15)
Figure 5: Results of decoding the content images with different combinations of phase structures: (a) $L_1/L_2=2/2$; (b) $L_1/L_2=4/2$; (c) $L_1/L_2=8/2$; (d) $L_1/L_2=2/4$; (e) $L_1/L_2=4/4$; (f) $L_1/L_2=8/4$; (g) $L_1/L_2=2/8$; (h) $L_1/L_2=4/8$; (i) $L_1/L_2=8/8$.

Table 1: Evaluation of decoding quality with different combinations of phase structures

<table>
<thead>
<tr>
<th>Phase level $L_1 / L_2$</th>
<th>2 / 2</th>
<th>4 / 2</th>
<th>8 / 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_r$</td>
<td>0.9890</td>
<td>0.9767</td>
<td>0.9794</td>
</tr>
<tr>
<td>$Q$</td>
<td>1.5061</td>
<td>0.8028</td>
<td>0.9220</td>
</tr>
<tr>
<td>$\eta$</td>
<td>0.3574</td>
<td>0.7061</td>
<td>0.8227</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase level $L_1 / L_2$</th>
<th>2 / 4</th>
<th>4 / 4</th>
<th>8 / 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_r$</td>
<td>0.9337</td>
<td>0.9699</td>
<td>0.9735</td>
</tr>
<tr>
<td>$Q$</td>
<td>0.5223</td>
<td>0.8018</td>
<td>0.9439</td>
</tr>
<tr>
<td>$\eta$</td>
<td>0.3574</td>
<td>0.7061</td>
<td>0.8227</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase level $L_1 / L_2$</th>
<th>2 / 8</th>
<th>4 / 8</th>
<th>8 / 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_r$</td>
<td>0.9406</td>
<td>0.9763</td>
<td>0.9784</td>
</tr>
<tr>
<td>$Q$</td>
<td>0.4845</td>
<td>0.7775</td>
<td>0.9163</td>
</tr>
<tr>
<td>$\eta$</td>
<td>0.3574</td>
<td>0.7061</td>
<td>0.8227</td>
</tr>
</tbody>
</table>

Figure 6: Decoding result after different shifting pixels between phase key and the watermarked image in X-axis in the case of $L_1/L_2=2/2$: (a) definition of X-axis and Y-axis; (b) shift 1 pixel; (c) shift 2 pixels.

In the following discussion, the algorithm has been taken by using 20 iteration cycles and let $\alpha$ equal to 0.15. Fig. 5(a)-5(j) and the corresponding datum in Table 1 verify the conclusion in Sec. 2 that the combination of 2/2 has the optimal quality of retrieval watermark and highest extracting efficiency. We also use other color host images, and the conclusions are identical.
4.2 Properties of binary phase watermark

The technique we present allows shifting of phase key and watermarked image in certain degree. Computer simulations are performed to illustrate the shifting property. We define horizontal axis and vertical axis as X and Y respectively which is also illustrated by Fig. 6(a). Fig. 6(b)-6(c) show the extracted image of shifting 1-2 pixels in X-axis. And the results of shifting 1-8 pixels in Y-axis are given in Fig. 7(a)-7(j). The corresponding measurement parameters are shown by Fig. 8(a) and 8(b). The same experiment is repeated, but with different key. In a word, the shifting pixels of phase key are inverse proportional to spatial sizes of key. In addition, we claim that extracted image has perfect quality when \( C_r > 0.95; Q > 0.75 \) and cannot be extracted when \( C_r < 0.9 \) according to the figures and datum referred above.

There is no optimum value for \( \alpha \), but the selection of \( \alpha \) must keep the appearance of the host image unchanged and the ability to recover the hidden image under severe distortion such as printing. Generally, the value of \( \alpha \) is 5%-15% in case of color host image processed by computer and it may be increased to 15%-20% in color printing. In this paper, the value of \( \alpha \) is 0.15.

The binary phase watermark is robust against A/D and D/A conversions during printing and scanning. We experiment with the popular devices such as Hp 3323 inkjet printer, Hp 5100 laser printer and microtek 4850 scanner. The printing/scanning process can result in the variation of pixel values and the geometric distortion. Before decoding,
we adjust the scanned image to the same size as the original, considering the following operation: rotation, shearing, trimming and scaling. The optical resolutions of printer and scanner are 360 dpi and 96 dpi, respectively. The scanned image is $604 \times 605$ pixels, and then adjusted to $256 \times 256$ pixels[see Fig. 9(a)]. The hidden image extracted from the watermarked image after printing and scanning is illustrated in Fig. 9(b).

Reducing the size of watermarked image will degrade the quality of extracted hidden image. It is also emphasize that, since the proposed method based on a holographic technique, the hidden information cannot be removed from the watermarked image, even if a fraction of it. Therefore, the watermark is also robust against cropping and coping.

![Figure 9: results after hard output (a) watermarked image after printing and scanning; (b) extracted image.](image)

### 4.3 Software design tool

On the basis of the above-discussed algorithmic procedures, an integrated software tool for watermark technology has been developed. The interface is shown in Fig. 10 (a) and 10(b), and the coder is based on VC 6.0. It can produce the on-line unique private key by choosing the option, random key, which is of high security. And it is helpful to validate the results quickly. We will perfect the software and make it practical in the future.

![Figure 10: (a) the interface of encoding process (b) the interface of decoding process](image)

### 5. CONCLUSIONS

Binary optics method has been applied to digital watermarking. Theory modeling verifies that the combined binary phase watermark is very secure and the extracted image has optimal quality in the case of 2/2 level combination. This method has feature of supporting the hard output of the watermarked image. Therefore, the digital watermarking with double binary phase encoding will be useful for information hiding and transferring.

### REFERENCES