A Robust Digital Watermarking in Geometric Attacks

Kyu-Tae Kim\textsuperscript{a}, Jin-Hyug Choi\textsuperscript{a}, Soo-Gil Kim\textsuperscript{b}, Jong-Uk Choi\textsuperscript{a,c}

\textsuperscript{a} MarkAny Research Institute, 10F, Ssanglim bldg, 151-11, Ssanglim-Dong, Chung-Gu, Seoul, 100-400, Korea
\textsuperscript{b} School of Electrical Engineering, Hoseo Univ., San 29-1, SeChul-Ri, BaeBang-Myun, Asan, 336-795, Korea
\textsuperscript{c} Div. of Computer Software, SangMyung Univ., 7 Hongji-Dong, Jongno-Gu, Seoul, 110-743, Korea

ABSTRACT

We propose a new watermarking scheme that can be used to embed multiple bits and also resilient to JPEG compression and geometrical transforms such as scaling, rotation, and cropping, based on holographic watermark that allows multiple watermark recovery without original content (cover image). The holographic watermark is that Fourier transformed digital hologram, embedded into cover image in the spatial domain. The proposed method has not only increased robustness with a stronger embedding but also imperceptibility of the watermark in the evaluation process. To compare with the conventional scheme, the spread spectrum, we embedded and recovered maximum 1,024 bits that consist of binary number over PSNR (peak signal-to-noise ratio) 39dB. And also, we computed robustness with BER (bit-error rate) corresponding the above attacks.

Keywords: image watermarking, digital hologram, copy protection, watermark robustness, geometrical transform

1. INTRODUCTION

Internet newspaper, e-magazine, e-book, TV, Video, and MP3 are considered as the assets of company to run e-business. However, lack of awareness or need for countermeasures against theft of materials in meaning of duplication causes huge impact on company revenue. Watermarking is to embed "hidden information" into text, image, video and audio that cannot be noticeable by human visual and auditory system. It can only be differentiated and known by a copyright holder though the network. It is a tool that marks hidden information into the multimedia content for copyright purpose. Later, watermark is extracted to use as concrete evidence of copyright ownership that used against for those who violated commercial ownerships.

* jedam@markany.com; phone 82-2-2262-5222; fax 82-2-2262-5333; markany.com
Practical watermarking schemes must make a trade-off between robustness from any kind of attacks and highly data payload with imperceptibility. General watermark attacks can be classified into JPEG compression and geometrical transformations such as rotation, scaling, and cropping. Spread spectrum schemes for watermarking purposes allow a low-energy signal to be embedded in each one of the frequency bands with a very low cross-correlation and is resistant to cropping, non-linear distortions of amplitude modulation and additive noise,\textsuperscript{1-3} but there are some drawbacks in synchronization. In this paper, it is not necessary to embed template to search synchronization during the watermark extraction process. The log-log mapping and log-polar map methods suggested to achieve scale and rotation invariance may not recover the watermark after a change of the aspect ratio. Furthermore, the overall robustness is not very good, since the watermark is embedded only in the amplitude of the Fourier transform.\textsuperscript{4-6} The schemes of template matching and auto-correlation function can estimate the affined distortion applied to the image by comparing the configuration of the extracted peaks with their expected configuration.\textsuperscript{7-8} The limitation of the those methods is the complexity, since it has to compute several times Fourier transform in the translation recovery process.

In this paper we present a new approach that uses the digital hologram as the watermark. We call it as the holographic watermark, which is resilient to JPEG compression and geometrical transformations. The proposed holographic watermark is satisfied with the trade-off between robustness and the competing requirements such as imperceptibility and information rate(payload) since hologram has redundancy and geometrical diffraction by nature. A hologram is recorded in interference pattern whose changing the rotation and the scale can make the diffracted light skew horizontally left or right with respect to the vertical axis. Since these two factors only alter the original position of the diffracted light, the proposed holographic watermark can recover the embedded data from geometrical transformations. And also the redundancy of the hologram can recover the original data from a partial hologram and then the holographic watermark is resilient to a cropping attack. In our simulations, we have made diffuse-type holographic watermark that is used in digital image processing by random phase modulation to reduce the strength of embedded data. To investigate the characteristics of the holographic watermark, we firstly compute the holographic watermark using a binary data stream and then embed it in ‘lena’ image with size of 256\times 256 pixels in the spatial domain. We analyze the holographic robustness to geometrical attacks using binary data of 90 bits and show recovery of embedded 1,024 bits binary data without bit error as the least image quality is 39dB.

2. BASICS OF FOURIER HOLOGRAM

In 1948, D. Gabor proposed a novel lensless imaging process, which we know as holography. Leith and Upatnieks suggested offset-reference hologram that solved twin image problem of Gabor’s hologram.

The reference wave from a reference point is collimated by the Fourier lens and strikes the object wave from an object point. These two waves are superposed on recording medium and then recorded on intensity pattern of the resultant field, which is called hologram. The hologram is added to object point’s intensity pattern since each object point construct independent intensity pattern by above process. We used one object point like one bit data which number and...
coordinate effects energy level of embedding hologram pattern in this paper. We can recover embedding bit data using the Fourier transform of the product of the hologram and reference wave.

When the embedding bit data (object point) and reference point are denoted by \( o(x_o, y_o) \) and \( r(x_r, y_r) \) respectively, these can be superposed as Eq. (1) in recording medium,

\[
U(\xi, \eta) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} o(x-x_o, y-y_o) \exp[-j \frac{2\pi}{\lambda_o f} (\xi x + \eta y)] d\xi d\eta \\
+ \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} r(x-x_r, y-y_r) \exp[-j \frac{2\pi}{\lambda_r f} (\xi x + \eta y)] d\xi d\eta \\
= O(\xi, \eta) \exp[-j \frac{2\pi}{\lambda_o f} (\xi x_o + \eta y_o)] + R(\xi, \eta) \exp[-j \frac{2\pi}{\lambda_r f} (\xi x_r + \eta y_r)],
\]

where the first term is the Fourier transform of bit data, \( (x_o, y_o) \), and the second term is the Fourier transform of reference, \( (x_r, y_r) \). The parameters \( \lambda_o \) and \( f \) indicate the wavelength and focal length of the recording process, respectively. The corresponding intensity distribution in the pattern between two waves of Eq. (1) is given by,

\[
U_h(\xi, \eta) = |O(\xi, \eta)|^2 + |R(\xi, \eta)|^2 \\
+ O(\xi, \eta)^* R(\xi, \eta) \exp[-j \frac{2\pi}{\lambda_o f} (\xi x_o + \eta y_o) + j \frac{2\pi}{\lambda_r f} (\xi x_r + \eta y_r)] \\
+ O(\xi, \eta) R(\xi, \eta)^* \exp[+j \frac{2\pi}{\lambda_o f} (\xi x_o + \eta y_o) - j \frac{2\pi}{\lambda_r f} (\xi x_r + \eta y_r)],
\]

where * indicates the complex conjugate. This expression is called the hologram whose the intensity depends on both the amplitude and the phase of the integrated object points that are embedding bit rates. We have only used the third and fourth terms on the right hand side of Eq. (2) because the first and second terms result in no images in the reconstruction. When the reconstruction wave (point) is denoted by \( (x_r', y_r') \), its complex wave can be written as,

\[
U_h(\xi, \eta) = R(\xi, \eta) \exp[-j \frac{2\pi}{\lambda_z f} (\xi x_r' + \eta y_r')],
\]

where the parameters \( \lambda_z \) and \( f' \) indicate the wavelength and focal length of the reconstruction process respectively.

Two waves are reconstructed when hologram is multiplied with reconstruction wave by Eq. (3). These reconstructed waves are converging or diverging from points. It remains to determine the exact locations of these real or virtual points of convergence. If the wavelength and focal length of the reconstruction process are the same as recording, the reconstructed waves are given by,
where the coordinates \((x_i, y_i)\) is the reconstructed bit data from the hologram. We conclude that the location \(x_i\) and \(y_i\) of the reconstructed bit data from the coefficients of the quadratic terms in \(x\) and \(y\). Eq. (5) provides the fundamental relations that allow us to predict the locations of the reconstructed bit data,

\[
\begin{align*}
\begin{cases}
  x_i = \mp x_0 \pm x_r
  \\
  y_i = \mp y_0 \pm y_r
\end{cases}
\end{align*}
\]

where the upper set of signs applies for one bit data and the lower set of signs for the other in hologram. Two sets from Eq. (5) are reconstructed the virtual and real image which lie to the left and right of the hologram, respectively. The hologram has uniform intensity distribution and the reconstructed image has symmetric twin-image.

3. PRINCIPLES OF THE PROPOSED HOLOGRAPHIC WATERMARK

In this paper we present a new approach that the digital hologram is used as the watermark. The proposed holographic watermark is resilient to JPEG compression and geometrical transformations such as rotation, scaling, and cropping. And also the holographic watermark is satisfied with embedding bit data and watermark perceptibility at the same time because the hologram strength is not augmented by the increased amount of embedded bit data. While most previous watermarking methods require the original image for recovery, the holographic watermark does not require the original image.

Now we describe application of the holographic watermark to conventional watermarking. As shown in above the hologram process, an embedded bit data is recorded in the Fourier hologram. This hologram is multiplied by weighting value \(\alpha\), so that the holographic watermark cannot be recognized. The proposed holographic watermark can be realized by superposing the weighted hologram onto the content image in spatial domain. Watermarked image \(w(x, y)\) can be expressed as follows.

\[
w(x, y) = c(x, y) + \alpha H(\xi, \eta),
\]
where \( c(x,y) \) and \( H(\xi, \eta) \) indicate a content image and the holographic watermark. The proposed method does not need to embed multiple cross shapes by Gruhl and Bender or a calibration signal in the Fourier domain patented by Digimarc corporation so that watermark resist to geometrical transformations. It is possible to reduce computation time and the loss of embedded data by transformation domain since the holographic watermark can be only used to determine the geometrical distortions without additive information. And also, the partial holographic watermark can recover fully the embedded data because of the redundancy of hologram, and it is especially robust to cropping and cutting distortions.

We can recover the embedded bit data using Fourier transform of watermarked image multiplied by the reconstructed wave in Eq. (3). The embedded bit data \( d(x_s, y_s) \) and the recovered bit data \( d(x_i, y_i) \) ’s relationship can be expressed by,

\[
d(x_s, y_s) = \sum_{n} d_i(x_s, y_s),
\]

\[
d(x_i, y_i) = \int \int w(x_s, y_s)U_k(\xi, \eta) \exp[j 2\pi(\xi x_i + \eta y_i)] d\xi d\eta,
\]

where \( N \) is number of embedding bit data. The Fourier transform of Eq. (8) is reconstructed with three components, which are the recovered real and virtual bit data, and the Fourier spectrum of the content image. We must separate the reconstructed bit data from the Fourier spectrum of the content image that disturbs recovering bit data. We should block a low frequency region using window mask like Fig. 1(c) and make the bit data recover in the high frequency region since the Fourier spectrum is generally concentrated in a low frequency region. The embedded bit data can be recovered only using window mask without the original content. Fig. 1(b) is watermarked image of the holographic watermark by an embedding image in Fig. 1(a). The recovered image and window mask is shown in Fig. 1(c). The size of window mask depends on the region of the embedding data. The bit data consists of multiple binary data stream as “1” and “0” in this experiments so that the holographic watermark can be applied for biometric information and two-dimensional barcode.
As seen in Fig. 2, the holographic watermark can embed and recover multiple bits without the original content image. To show the holographic watermark’s ability to embed a great number of bits, 80 bits of Fig. 2(a) have been used as a watermark to be embedded in the content image with 45dB. The start and end pixel points of the embedding bits are (20, 100) and (105, 120) respectively, and a reference and reconstruction point are (129, 129). The holographic watermark of Fig. 2(b) is made by each bit of Fig. 2(a) and then multiplied by weighting value not to distinguish visually from the content image. As seen in Fig. 2(b), the holographic watermark is constructed to have a uniform intensity distribution as a whole by using random phase modulator which can improve the quality of watermarked image and the recovered data. The embedded data is multiplied by random phase modulator before it is Fourier transformed and then superposed by a reference point. But the recovered data is obtained independently of the random phase modulator. The recovered bits seen in Fig. 2(d) appeared in different regions that one recovers from (20, 100) to (105, 120) and the other recovers from (238, 159) to (153, 139) according to Eq. (5).

One pixel is one bit displayed by “0” and “1” and therefore we can embed the bit data as much as the size of a content image except the size of a window mask of Fig. 1(c). The embedding bit data can be recovered without error in an simulation when the size of window mask is half a content image and under. The embedding capacity of the holographic watermark has the maximum 256×128 bits when a content image is the size of 256×256 like Fig. 2.

4. SIMULATION RESULTS AND ANALYSIS

The digital watermark must be available not only to the more information but also to robustness of the distortions and attacks. The main problems are geometrical transformations and lossy compression. In our case the holographic watermark has to resolve the above problems. To investigate the effect of using the holographic watermark, the holographic watermark with size of 256×256 is given by a binary data, which was evaluated after geographical transformations and JPEG compression. The robustness is usually measured by the BER(bit-error ratio), defined as the ratio of wrong recovered bits to the total number of embedded bits.
By changing the orientation of the hologram the diffracted wave can be made to skew horizontally left and right with respect to the vertical axis. To test the holographic watermark for rotation attack, the 8 bit gray scale of “lena” image, 256×256 pixels in size, was watermarked with PSNR 44dB. Fig. 3 is the results of the recovered bits from the holographic watermark that is rotated from 15 to 90 degrees. As shown in Fig. 3, rotating attack may be recognized correctly by gradient of the recovered bits because it is the same as a rotated angle of the watermarked image. However, the modified image shown in Fig. 3(b) has to be reversed to obtain the correct results. Fig. 3(c), (d), (e), and (f) are the recovered bits at different locations, although bit error may be arose from a rotating angle of watermarked image.

Fig. 3. Rotation attacks. Recovered bits are (c) 30, (d) 90 degrees in a counterclockwise direction

Fig. 4 shows the recovered bits from a distorted watermarked image after inverse geometrical transform. If the inverse transform brought distorted image to right direction, the embedded bits will be recovered without bit error as shown in Fig. 4(a). Faulty inverse may lead to bit error such as Fig. 4(b)

Fig. 4. Recovered bits from the reversed watermarked image

The diffraction angle of the hologram is determined by the spatial frequency. The spatial frequency of the hologram i.e. the number of interference fringes per mm can be adjusted. This is achieved by changing the angle between the reference and object waves. However, a scaling distortion of the hologram also causes the spatial frequency to change since it is the same as a changing distance between interference fringes. If the original hologram decreases in size, the
number of interference fringes increases with the spatial frequency and a decrease in the hologram magnifies a diffraction angle of reconstruction image.

Fig. 5 is the result of the embedding bits recovered from a decrease and increase in watermarked images. It is seen in the Fig. 5 that the embedding bits are recovered for different images 256×256 (×1, original image), 128×128 (×0.5), and 512×512 (×2) pixels in size, although the recovered bits have a different distance between twice and a half from 15 pixels. In this way it has been verified that the holographic watermark can still be recovered from the scale distortions of watermarked image. The recovered bits of Fig. 5(b) magnify 30 pixels with a decrease in watermarked image size and Fig. 5(c) demagnifies 7 pixels with an increase in size. The scale effects of the holographic watermark can be found from the Eq. (5) derived above for bits locations as shown in Eq. (11),

\[ M = \left| \frac{\partial \phi}{\partial \phi_0} \right| = \left| \frac{\partial \phi}{\partial \phi_r} \right| = \left| \frac{\partial \phi}{\partial \phi_f} \right| = m \left| 1 - \frac{f}{f'} \mp m \frac{\lambda_f}{\lambda_f} \right|^2 \tag{11} \]

where \( m \) and \( M \) are scale factor of the holographic watermark and recovered bit, respectively. If \( m \) is the demagnification (\( m < 1 \)) to which the holographic watermark, then we can see that embedded bits are recovered with magnification as shown in the Fig. 5(b). The holographic watermark is especially to robust to magnification (\( m > 1 \)) so that the error ratio of the recovered bits is lower than demagnification.

Fig. 5. Recovered bits by (a) original size, (b) demagnification, and (c) magnification of holographic watermark.

Fig. 6 is result of the recovered bits that was realized from watermarked images with the various scale distortions of 60~200%. The holographic watermark can be correctly recovered by 90% scale distortion above 40dB. The recovered bits may be seen for 60% scale, although BER increases with a decrease in size. In this way it has been verified that the holographic watermark can still be recovered from the scale distortion.
Fig. 6. Recovered bits with (a) >90% (b) 80% (c) 70% (d) 60% scales in watermarked image size.

Fig. 7 shows BER of the holographic watermark that was transformed by scaling attack. It was performed on size of 256×256 pixels, 90 bits inserted. This graph allows immediate evaluation of the allowable the scaling attack of the holographic watermark for given BER. It is especially useful in case that BER range is given and corresponding maximal allowable scaling distortion needs to be evaluated. And also, we can see robustness(BER) comparisons for a given visual image quality which depends upon a strength in the holographic watermark. An image of PSNR 39dB may be taken a suitable trade-off between robustness and visual quality, in that case Fig. 7 shows 3.3% bit error under with respect to 60% scaling attack.

Fig. 7. BER vs. scaling attack for the holographic watermark

The holographic watermark is robust to a cropping distortion because hologram has an abundant redundancy by nature. To investigate the effect of cropping images, watermarked images were cropped from the original images with size of 256×256 pixels. Fig. 8 is result of the recovered bits from watermarked image with a cropping attack. Payload 90 bits were inserted in watermarked image and a visual quality was kept up PSNR 39dB. It is seen in the Fig. 8, that the recovered image may be recognized for partial images 128×128(50%) and 100×100(40%) pixels, respectively, although BER increased with a decrease in image size. Fig. 9 shows robustness(BER) vs. cropping attacks for a proposed method. It was performed on size of 256×256 pixels, 90 bits inserted. For a given cropping, Fig. 9 can be used in determining...
the expected BER for a desired visual quality. The images of PSNR 44dB and 39dB were detected 20% and 2.2% bit error, respectively, with the cropped size of 100×100 pixels.

![Images of PSNR 44dB and 39dB with corresponding cropped sizes](image)

**Fig. 8.** Cropping images and recovered bits for payload 90 bits and PSNR 39dB. Image sizes are (a) 128×128 (50%) and (b) 100×100 (40%) pixels and recovered bits are (c) 128×128 and (d) 100×100.

![Graph showing BER from cropping attack](graph)

**Fig. 9.** BER vs. cropping attack for the holographic watermark

JPEG compression is currently the most widely used compression algorithm for still image. For image watermarking, we need a method that is resilient to JPEG compression with high compression factor. It is usually more efficient to employ a method in a transform domain than a spatial domain. Similarly, spatial domain methods are probably more suitable for geometrical distortions. Although the holographic watermark is realized in a spatial domain, it is resilient to JPEG compression. Fig. 10 is result of the recovered from JPEG image for high compression QF (quality-factor). Set the quality of the compressed image to a value between 0 and 100. This only affects compression. Fig. 10(a) shows JPEG image of PSNR 44dB that was compressed by QF 10. We got recovered bits without error as shown in Fig. 10(b).

![JPEG image and recovered image](image)

**Fig. 10.** JPEG image and recovered image for proposed method.

JPEG is most widely used procedure to store and send digital image. The JPEG provides a high compression ratio and desired quality. Fig. 11 shows robustness (BER) vs. JPEG compression for a proposed method. It was also performed on size of 256×256 pixels, 90 bits inserted. For high compressed watermarked image, the holographic watermark can be recovered without detection error. BER was detected less than 1% in PSNR 44dB of QF10 images as shown in Fig. 11.
5. CONCLUSION

In this paper we propose a new digital watermarking scheme for copyright protection. Holographic watermark allows multiple watermark recovery without original cover image, even if watermarked image was distorted by lossy compression and generalized geometrical transforms such as rotation, scaling, and cropping. From the theoretical analysis and simulation results, the proposed method is fit for watermarking applications and requirements. For watermark embedding strength, we embedded and recovered maximum 1,024 bits that consist of binary number over PSNR 39dB. As a geometrical robustness we use a BER defined as the ratio of wrong expected bits to the total number of embedded bits. All experiments (simulations?) were performed on the 256×256 pixels, and 8bit gray scale of ‘lena’. And also watermark payload was 90 bits with different PSNR 39dB and 44dB. Simulation results showed that our proposed method is very robust to JPEG compression and all geometrical distortions not more than 20% when numeric measurement of visual quality indicates by PSNR > 44dB on average. Even 50% distorted image can be recovered without error in all the BER vs. attacks graph if quality illustrates PSNR >39dB. For high compressed watermarked
image, the holographic watermark can be recovered without detection error. Bit error was detected less than 1% in PSNR 44dB of QF10 images. Though this paper is limited in generalized geometrical attacks and JPEG compression, the further study to increase the robustness about different attack such as D/A and A/D conversion for off-line protection will be performed in the future.

Acknowledgement

This research has been conducted by 2000N-NL-01-C-296 Program’s supporting.

6. REFERENCES