

**中国版权保护中心计算机软件著作权登记申请补正通知书 [\*\*\*\*\*]**

发件人: cpccmail@ccopyright.com<cpccmail@ccopyright.com>

时 间: 2019年11月20日(星期三) 下午3:59

收件人: Hollow Man<\*\*\*\*\*>

**软件登记补正通知书**

流 水 号: \*\*\*\*\*

软件全称: Hollow 图片(视频) 信息隐藏加解密软件

版 本 号: V1.0

登记类型: 计算机软件著作权登记申请

申 请 人: Hollow Man

经审查, 上述软件登记申请文件存在下列缺陷。根据《计算机软件著作权登记办法》第二十二条之规定, 申请人应于收到本通知之日起日内予以补正, 逾期未补正, 视为撤回申请。

缺陷及须补正的内容如下:

文档截图中出现兰州大学, 并说是基于蔡铭峯等人的研究成果\*\*\*\*, 请书面说明综合与本软件的关系(所涉及到的主体签字、盖章), 明确权利归属

\*\*\*\*\*重要提示: 请将此补正通知书邮件打印, 并附在补正材料第一页(不要装订), 邮寄或直接送至“302软件登记部 补正组”收, 否则会造成材料丢失或办理流程的延误

\*\*\*\*\*如有问题请联系补正组 (010- 84195640) \*\*\*\*\*

以上缺陷, 请提交符合要求的材料一式一份。

中国版权保护中心软件登记部

2019 年11 月20 日

审查员: 王春晓 email地址: wangchunxiao@ccopyright.com

通讯地址: 北京市西城区天桥南大街1号天桥艺术大厦A座三层302室软件登记部 邮编: 100050

软件登记部 补正组：

您好！

关于补正通知书中所述，软件作者本人做出以下几点陈述：

1. 本软件基于蔡铭峯等人的研究成果，指的是基于以台湾國立高雄應用科技大學的蔡铭峯 (Ming-Feng Tsai) 为第二作者的论文” High-capacity Robust Watermarking Approach for Protecting Ownership Right” 中所述信息隐藏加密算法思路 (论文见附件一). 本人基于该算法思路编写代码, 实现并完成了我的” Hollow 图片 (视频) 信息隐藏加解密软件” 编写, 并且本人通过互联网渠道获取到该论文, 与蔡铭峯等人并无联系渠道和任何合作关系, 蔡铭峯等人也未直接帮助本软件的代码编写, 仅起到算法部分的启示作用. 且程序中” 关于作者” 这一部分已经明确到了这一点：



2. 因软件作者本人为兰州大学在读学生，因而在代码中标注了作者本人学校的个人信息.
3. 另在申请文档中的” 设计说明书” 引言部分第 3 小节” 参考资料” 中已经标注出了蔡铭峯等人对本软件算法部分的启示作用，” 设计说明书” 的引用如下：

本软件的图片加密解密算法参考了这篇论文： Hsiao CY., Tsai MF., Yang CY. (2017) High capacity Robust Watermarking Approach for Protecting Ownership Right. In: Pan JS., Tsai PW., Huang HC. (eds) Advances in Intelligent Information Hiding and Multimedia Signal Processing. Smart Innovation, Systems and Technologies, vol 63. Springer, Cham.

附件：

1. 蔡铭峯等人的论文” High-capacity Robust Watermarking Approach for Protecting Ownership Right”
2. 作者本人的兰州大学在读证明.

软件作者本人签名：

*Hollow Man*

# High-capacity Robust Watermarking Approach for Protecting Ownership Right

Chun-Yuan Hsiao<sup>1</sup>, Ming-Feng Tsai<sup>1</sup>, and Ching-Yu Yang<sup>2</sup> \*

Dept. of Computer Science and Information Engineering

<sup>1</sup>National Kaoshiung University of Applied Science, Taiwan

cyhsiao@kuas.edu.tw, 1104308106@gm.kuas.edu.tw

Dept. of Computer Science and Information Engineering

<sup>2</sup>National Penghu University of Science and Technology, Taiwan

chingyu@gms.npu.edu.tw

**Abstract.** In this work, we proposed a high-capacity robust watermarking scheme for color images. Based on integer wavelet domain (IWT), the proposed scheme utilized the idea of computing the offset of two square-root-values, a number of data bits can be embedded in a host image. Simulations indicated that our method did provide a large hiding-storage while the perceived quality is good. Further, the proposed method is tolerant of various attacks such as brightness, cropping, edge sharpening, blurring, flip horizontal, inversion, and rotation. Additionally, the payload for the proposed method is larger than that for existing techniques.

**Keywords:** Data hiding, high-capacity robust watermarking, steganography.

## 1 Introduction

With the proliferation of Industry 4.0, or the fourth industrial revolution, the trend of automation and data exchange in manufacturing technologies is ubiquitous around the world. Namely, the organizations can effectively achieve their business goals by using the platform, which composed of internet of thing (IOT), intelligent robot (IR), cloud computing, and big data analytics. Consequently, the individuals and parties are easily to share their secret (or private) information from the Internet. However, data could be eavesdropped or tampered with during transmission. Data hiding can provide an economic ways to against the above issues. Generally, data hiding can be classified into two categories: steganography and digital watermarking [1, 2]. The steganographic methods provide a high payload with good perceived distortion, whereas robustness is the major goal of watermarking schemes. Recently, several researchers have presented their watermarking approaches for protecting copyright and ownership in color images [3–6]. However, either hiding capacity or robustness is not good enough. In this paper, we propose a high-capacity robust digital watermarking to achieve the goal.

---

\* To whom correspondence should be addressed.

## 2 Proposed Method

To achieve a high-capacity robust approach, we only embed data bits into the high-high (HH) subband of the level 1 (L1) of integer wavelet transform (IWT) domain. Namely, prior to bit embedment, an input image is decomposed to the IWT domain by using the following two formulas:

$$d_{j,k} = s_{j-1,2k+1} - s_{j-1,2k} \quad (1)$$

and

$$s_{j,k} = s_{j-1,2k} + \left\lfloor \frac{d_{j,k}}{2} \right\rfloor \quad (2)$$

where  $s_{j,k}$  and  $d_{j,k}$  are the  $k$ -th low-frequency and high-frequency wavelet coefficients at the  $j$ -th level, respectively [7]. The  $\lfloor x \rfloor$  is a floor function. The details of the scheme are described in the following sections.

### A. Bit Embedding

Without loss of generality, let  $W_j = \{(w_{rj}, w_{gj}, w_{bj})\}_{j=0}^{ab-1}$  be the  $j$ -th pixel derived from an input (scrambled) watermark of size  $a \times b$ . Also let  $C = \{(c_{rj}, c_{gj}, c_{bj})\}_{j=0}^{ab-1}$  with  $c_{rj} = \sqrt{w_{rj}} - \text{round}(\sqrt{w_{rj}})$ ,  $c_{gj} = \sqrt{w_{gj}} - \text{round}(\sqrt{w_{gj}})$ , and  $c_{bj} = \sqrt{w_{bj}} - \text{round}(\sqrt{w_{bj}})$  be the three deviation values of  $W_j$ . The main procedure of bit embedding is specified in the following algorithm.

Algorithm 1. Hiding data bits in an RGB color image.

Input: A host color image  $S = \{(r_i, g_i, b_i) | i = 1, 2, \dots, MN\}$  and a scrambled watermark  $W$ .

Output: A marked image  $\hat{S}$  with an auxiliary set of parameters  $C$ .

Method:

Step 0. Perform L1 IWT from host image  $S$  to obtain the HH-subband  $H = \{(h_{rj}, h_{gj}, h_{bj})\}_{j=0}^{(MN/4)-1}$  of IWT coefficients.

Step 1. Input a set of coefficient  $H_j$  which derived from  $H$ . If the end of input is encountered, then proceed to Step 11.

Step 2. Assign a sign mark  $s_{rj} = 1$  if  $h_{rj} > 0$ ,  $s_{gj} = 1$  if  $h_{gj} > 0$ , and  $s_{bj} = 1$  if  $h_{bj} > 0$ , respectively, and go to Step 3. Otherwise, assign  $s_{rj} = -1$  if  $h_{rj} \leq 0$ ,  $s_{gj} = -1$  if  $h_{gj} \leq 0$ , and  $s_{bj} = -1$  if  $h_{bj} \leq 0$  and get the absolute values  $h_{rj} = |h_{rj}|$ ,  $h_{gj} = |h_{gj}|$ , and  $h_{bj} = |h_{bj}|$ , respectively.

Step 3. Round the values  $d_{rj} = \text{round}(\sqrt{w_{rj}})$ ,  $d_{gj} = \text{round}(\sqrt{w_{gj}})$ , and  $d_{bj} = \text{round}(\sqrt{w_{bj}})$ . In addition, calculate the deviation values  $c_{rj} = \sqrt{w_{rj}} - d_{rj}$ ,  $c_{gj} = \sqrt{w_{gj}} - d_{gj}$ , and  $c_{bj} = \sqrt{w_{bj}} - d_{bj}$  and save as an auxiliary information.

Step 4. Compute the values  $h_{rj} = \frac{[h_{rj} - (h_{rj} \bmod 10)]}{10}$ ,  $h_{gj} = \frac{[h_{gj} - (h_{gj} \bmod 10)]}{10}$ , and  $h_{bj} = \frac{[h_{bj} - (h_{bj} \bmod 10)]}{10}$ .

Step 5. Set flag  $\alpha = 1$ .

Step 6. Assign  $h_k = h_{rj}$ ,  $d_k = d_{rj}$ ,  $s_k = s_{rj}$  if  $\alpha = 1$ ;  $h_k = h_{gj}$ ,  $d_k = d_{gj}$ ,  $s_k = s_{gj}$  if  $\alpha = 2$ ; and  $h_k = h_{bj}$ ,  $d_k = d_{bj}$ ,  $s_k = s_{bj}$  if  $\alpha = 3$ , otherwise, if  $\alpha > 3$  then go to Step 1.

Step 7. If  $d_k \geq 10$ , then do the following substeps:

Step 7a. If  $(h_k \bmod 2) = 1$  then evaluate  $h_k = [(h_k - 1) \times 10] + (\frac{d_k}{10}) + d_k \bmod 10 \times s_k$  else  $h_k = [(h_k \times 10) + (\frac{d_k}{10}) + d_k \bmod 10] \times s_k$ .  
 Step 7b. Compute  $\alpha = \alpha + 1$  and go to Step 7.  
 Step 8. If  $d_k < 10$ , then do the following substeps:  
 Step 8a. If  $(h_k \bmod 2) = 1$  then compute  $h_k = (h_k \times 10 + d_k) \times s_k$ , else  $h_k = [(h_k + 1) \times 10 + d_k] \times s_k$ .  
 Step 8b. Compute  $\alpha = \alpha + 1$  and go to Step 6.  
 Step 9. Repeat Step 1 until all data bits have been processed.  
 Step 10. Perform inverse IWT from the (marked) IWT coefficients to obtain marked image  $\hat{S}$ .  
 Step 11. Stop.

## B. Data Extraction

The primary procedure of the proposed bit extraction is described in the following algorithm.

Algorithm 2. Extracting hidden bits from a marked image.

Input: A marked image  $\hat{S} = \{(\hat{r}_i, \hat{g}_i, \hat{b}_i) | i = 1, 2, \dots, MN\}$  and an auxiliary set of parameters  $C$ .

Output: An extracted watermark  $W' = \left\{ (w'_{rj}, w'_{gj}, w'_{bj}) \right\}_{j=0}^{ab-1}$

Method:

Step 0. Perform L1 IWT from marked image  $\hat{S}$  to obtain the HH-subband  $\hat{H} = \left\{ (\hat{h}_{rj}, \hat{h}_{gj}, \hat{h}_{bj}) \right\}_{j=0}^{(MN/4)-1}$  of IWT coefficients.

Step 1. Input a set of coefficient  $\hat{H}_j$ , which derived from  $\hat{H}$ . If the end of input is encountered, then proceed to Step 9.

Step 2. Set the marks  $s_{rj} = 1$  if  $\hat{h}_{rj} > 0$ ,  $s_{gj} = 1$  if  $\hat{h}_{gj} > 0$ , and  $s_{bj} = 1$  if  $\hat{h}_{bj} > 0$ , respectively, and go to Step 3. Otherwise, set  $s_{rj} = -1$  if  $\hat{h}_{rj} \leq 0$ ,  $s_{gj} = -1$  if  $\hat{h}_{gj} \leq 0$ , and  $s_{bj} = -1$  if  $\hat{h}_{bj} \leq 0$ ; besides, get the absolute values  $\hat{h}_{rj} = |\hat{h}_{rj}|$ ,  $\hat{h}_{gj} = |\hat{h}_{gj}|$ , and  $\hat{h}_{bj} = |\hat{h}_{bj}|$ , respectively.

Step 3. Compute the values  $w'_{rj} = \hat{h}_{rj} \bmod 10$ ,  $w'_{gj} = \hat{h}_{gj} \bmod 10$ , and  $w'_{bj} = \hat{h}_{bj} \bmod 10$ .

Step 4. Set flag  $\beta = 1$ .

Step 5. Obtain  $h_k = \hat{h}_{rj}$ ,  $w_k = w'_{rj}$ ,  $s_k = s_{rj}$ ,  $c_k = c_{rj}$  if  $\beta = 1$ ;  $h_k = \hat{h}_{gj}$ ,  $w_k = w'_{gj}$ ,  $s_k = s_{gj}$ ,  $c_k = c_{gj}$  if  $\beta = 2$ , and  $h_k = \hat{h}_{bj}$ ,  $w_k = w'_{bj}$ ,  $s_k = s_{bj}$ ,  $c_k = c_{bj}$  if  $\beta = 3$ , otherwise, if  $\beta > 3$  then go to Step 1.

Step 6. Compute the value  $T = \frac{(h_k - w_k)}{10}$ , if  $T \bmod 2 = 1$  then do nothing, otherwise evaluate  $w_k = w_k + 9$ .

Step 7. Evaluate  $w_k = (w_k + c_k)^2$ ,  $h_k = h_k \times s_k$ , and  $\beta = \beta + 1$ , respectively, go to Step 5.

Step 8. Repeat Step1 until all hidden bits have been extracted.

Step 9. Assemble, descrambled and form the watermark  $W'$ .

Step 10. Stop.

### C. Analysis and Discussion

As specified previously, without the help of auxiliary information, the extraction of the hidden watermark would be unsuccessfully at the receiver. However, the adversaries (or the third parties) are incapable of extracting hidden message if they have no auxiliary information. The optimal payload for our method is  $\frac{(4 \times 3 \times 256 \times 256)}{512 \times 512} = 3$  bpp (bit per pixel). The overhead  $C = \{(c_{rj}, c_{gj}, c_{bj})\}_{j=0}^{ab-1}$  for the proposed scheme is associated with the size of the watermark. In addition, each non-integer value in the set of  $(c_{rj}, c_{gj}, c_{bj})$  lies between -1.0 and +1.0. To reduce the transmission time and increase privacy, the overhead can be losslessly compressed by using either the run-length coding algorithm or JBIG2 [8]. The resultant coded data can then sent by an out-of-band transmission to the receiver.

## 3 Experimental Results

Four  $512 \times 512$  color images, as shown in Fig. 1, were used as host images. Each RGB pixel of the host images is represented by 24 bits, 8 bits per component. The size of the test color watermark is  $256 \times 256$ , as depicted in Fig. 2. The marked images generated by the proposed method are depicted in Fig. 3. It can be seen from the figure that the perceived quality is good. No apparent color distortion appeared in the figures. Their average PSNR is 42.42 dB. The PSNR is defined by

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \quad (3)$$

with  $MSE = \frac{(\sum_{i=1}^{MN} [(r_i - \hat{r}_i)^2 + (g_i - \hat{g}_i)^2 + (b_i - \hat{b}_i)^2])}{3MN}$ . Here  $(r_i, g_i, b_i)$  and  $(\hat{r}_i, \hat{g}_i, \hat{b}_i)$  denote the RGB pixel values of the host image and the marked image. Notice that an input watermark was fully embedded in the host images, namely, the bit rate for each marked images is  $\frac{(2 \times 3 \times 256 \times 256)}{512 \times 512} = 2.17$  bpp. Tradeoff between PSNR and payload for our method in four test image were shown in Fig. 4. The figure indicated that the PSNR performance for the image Goldhill is the best among test images, while Jet has the least PSNR as payload was larger than 1 bpp. Generally, the average PSNR of the test images has significantly increased when payload being less than 1 bpp.



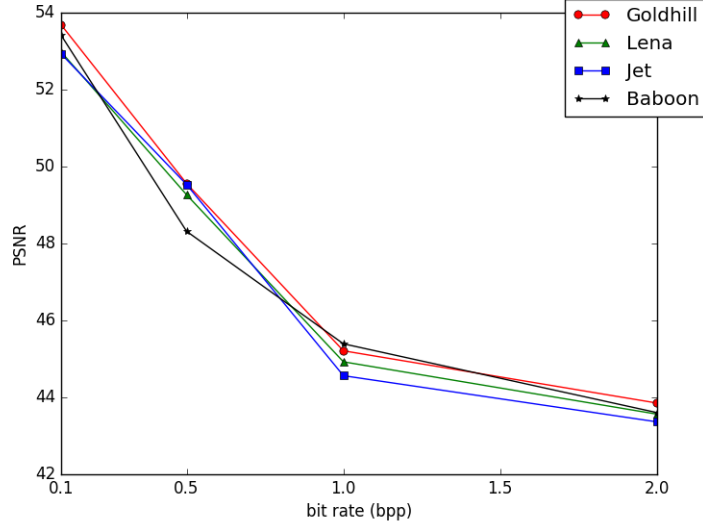
**Fig. 1.** The host images. (a) GoldHill, (b) Lena, (c) Jet, and (d) Baboon.



**Fig. 2.** The test watermark.



**Fig. 3.** The marked images generated by the proposed method. (a) GoldHill (PSNR=42.70 dB), (b) Lena (PSNR=42.53 dB), (c) Jet (PSNR=42.23 dB), and (d) Baboon (PSNR=42.35 dB).



**Fig. 4.** Trade-off between PSNR and payload for the proposed method.

To demonstrate the robustness of the proposed method, examples of extracted watermarks after various manipulations of the image were given in Table 1. The normalized correlation (NC) value is also included. The  $NC_{RGB}$  is defined by



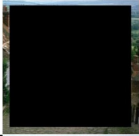
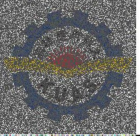










$$NC_{RGB} = \frac{NC_R + NC_G + NC_B}{3} \quad (4)$$

where  $NC_R = \frac{\sum_i \sum_j w_R(i,j)w_R'(i,j)}{\sum_i \sum_j [w_R(i,j)]^2}$ ,  $NC_G = \frac{\sum_i \sum_j w_G(i,j)w_G'(i,j)}{\sum_i \sum_j [w_G(i,j)]^2}$ , and  $NC_B = \frac{\sum_i \sum_j w_B(i,j)w_B'(i,j)}{\sum_i \sum_j [w_B(i,j)]^2}$ . Here  $w_R(i,j)$ ,  $w_G(i,j)$ , and  $w_B(i,j)$  as well as  $w_R'(i,j)$ ,  $w_G'(i,j)$ , and  $w_B'(i,j)$  denote the RGB pixel values of the original watermark and the extracted one, respectively.

From Table 1 we can see that most of the extracted watermarks are recognized. Although the  $NC_{RGB}$  of the extracted watermark which attacked by cutting off 80% from the marked image, it is identifiable. Notice as well the  $NC_{RGB}$  of the survived watermark extracted from a marked image, which had undergone inversion attack, is still recognizable. In addition, the extracted watermarks are recognized when the marked images were rotated by 90 degrees. Similar performance can be found in the marked images which manipulated by brightness. From the above demonstration, we concluded that the marked images generated by the proposed method do resist from attacks including edge sharpening, cropping, rotation, brightness, and inversion.



**Table 1.** The survived watermarks extracted from the marked images which undergone various manipulations.

Attacks	Distorted Image	Survived Watermark
<b>Attack free</b> $NC_{RGB}=0.99662$		
<b>Cropping 80%</b> $NC_{RGB} = 0.46536$		
<b>Edge crispening</b> $NC_{RGB} = 0.74151$		
<b>Rotate 90 degrees</b> $NC_{RGB} = 0.78016$		
<b>Brightness -100</b> $NC_{RGB} = 0.61653$		
<b>Negative</b> $NC_{RGB} = 0.99479$		
<b>Flip Horizontal</b> $NC_{RGB} = 0.77937$		

Performance comparison between the proposed method and existing schemes: Yang's scheme [3], Yang and Wang[5], and Yang and Wang[6] is given in Table 2. It is obvious that the proposed method provides the largest PSNR and payload among these compared methods. Also notice that the average payload for the proposed method is approximated eleven times larger than that for the Yang and Wangs techniques [5].

**Table 2.** PSNR/payload (bit) comparison of various methods.

Images	Payload (bit)/ PSNR (dB)			
	Yang [3]*	Yang and Wang [5]	Yang and Wang [6]	Our method
Lena	17,874/39.59	16,042/43.54	57,600/39.07	177,068/46.00
Baboon	15,474/39.61	15,373/39.40	57,600/29.39	177,068/45.05
Jet	21,345/39.34	16,309/42.74	57,600/39.17	177,068/45.76
House	17,146/39.21	16,660/48.44	57,600/47.35	177,068/44.37
Tiffany	21,872/37.50	16,403/43.23	57,600/39.64	177,068/43.02
Average	18,742/39.05	16,157/43.47	57,600/38.92	177,068/44.84

\*With the watermarking approach of Yang's technique.

## 4 Conclusion

By using the computation of the offset between two square-root-values, a large volume of secret bits can be successfully embedded in the host images by the proposed method. Experimental results confirmed that the perceptual quality of the marked images is good while the hiding-capacity is high. Moreover, the proposed method does resist several kinds of attacks such as brightness, cropping, edge sharpening, blurring, flip horizontal, inversion, and rotation. Additionally, the hiding-capacity of our proposed method is larger than that of existing techniques. Major applications of the proposed method can be found in the protection of copyright and ownership.

## References

1. I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd Ed., Morgan Kaufmann., MA, USA, 2008.
2. E. Eielinska, W. Mazurczyk, and K. Szczypiorski, Trends in steganography, *Communications of the ACM* 57, 86-95, 2014.
3. C.Y. Yang, Robust watermarking scheme based on radius weight mean and feature-embedding technique, *ETRI Journal*, vol. 35, pp. 512-522, 2013.
4. C.C. Lin, C.C. Chang and Y.H. Chen, A novel SVD-based watermarking scheme for protecting rightful ownership of digital images, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, pp. 124-143, 2014.
5. C.Y. Yang and W.F. Wang, Robust color image watermarking approach based on shape-specific points, *The 10th Int. Conf. on Intellig. Info. Hiding and Multim. Sig. Proc.*, Kitakyushu, Japan, Aug. 27-29, pp. 65-68, 2014.
6. C.Y. Yang and W.F. Wang, High-performance digital watermarking with L2-norm centroid for colour images, *The 11th Int. Conf. on Intellig. Info. Hiding and Multim. Sig. Proc.*, Adelaide, Australia, Sept. 23-25, pp. 29-31, 2015.
7. A. R. Calderbank, I. Daubechies, W. Sweldens, and B. L. Yeo, Wavelet transforms that map integers to integers, *Applied & Computational Harmonics Analysis*, vol. 5, no. 3, pp. 332-369, 1998.
8. P.G. Howard, F. Kossentini, B. Martins, S. Forchhammer, and W.J. Rucklidge, The emerging JBIG2 standard, *IEEE T. Circuits and Systems for Video Technology*, vol. 8, pp. 838-848, 1998.