A Wavelet Watermarking Algorithm Based on a Tree Structure

Oriol Guitart Pla^a , Eugene T. Lin^b, and Edward J. Delp^b

^aUniversitat Politecnica de Catalunya (UPC) Barcelona Spain

^bVideo and Image Processing Laboratory School of Electrical and Computer Engineering Purdue University West Lafayette, Indiana USA

ABSTRACT

We describe a blind watermarking technique for digital images. Our technique constructs an image-dependent watermark in the discrete wavelet transform (DWT) domain and inserts the watermark in the most significant coefficients of the image. The watermarked coefficients are determined by using the hierarchical tree structure induced by the DWT, similar in concept to embedded zerotree wavelet (EZW) compression. If the watermarked image is attacked or manipulated such that the set of significant coefficients is changed, the tree structure allows the correlation-based watermark detector to recover synchronization.

Our technique also uses a visual adaptive scheme to insert the watermark to minimize watermark perceptibility. The visual adaptive scheme also takes advantage of the tree structure. Finally, a template is inserted into the watermark to provide robustness against geometric attacks. The template detection uses the cross-ratio of four collinear points.

Keywords: Tree Structure, Perceptual Model, Watermarking

1. INTRODUCTION

There has been an explosion in the growth of multimedia distribution and communications in the past few years, creating a demand for content protection techniques.^{1, 2} Cryptographic systems provide security by scrambling the multimedia contents, but nothing prevents the user from manipulating or copying the decrypted data for illegal uses. In order to solve these issues, watermark algorithms have been proposed as a way to complement the encryption processes and provide some tools to track the retransmission and manipulation of multimedia contents.^{3, 4}

There are several ways to classify watermarking techniques. A watermarking technique which requires the original signal to detect the watermark is known as a *non-blind* technique. Conversely, a *blind* technique does not require access to the original signal for watermark detection. A watermarking technique may also be classified by how the watermark is inserted. Some watermarking techniques embed the watermark in the spatial domain while others embed the watermark in a transform domain, such as the discrete cosine transform (DCT) or discrete wavelet transform (DWT).⁵ Transform domain embedding may be more robust against image manipulation compared with spatial domain schemes.

There are some desirable characteristics of effective watermarking techniques, including imperceptibility, robustness, and security. Imperceptibility is the degree of perceptual similarity between the original and watermarked signals. It is desirable to embed the watermark in a discreet, unobtrusive manner so that the watermark is imperceptible under casual observation. Robustness is the resilience of the watermark against manipulations

This work was partially supported by the Air Force Research Laboratory, Information Directorate, Rome Research Site, under research grant number F30602-02-2-0199. Address all correspondence to E. J. Delp at ace@ecn.purdue.edu.

such as lossy compression, linear and non-linear filtering, scaling, and cropping. Security is the ability of the watermark to resist hostile attacks. Attacks are not limited to removal of the watermark, but include watermark estimation or forgery, collusion, and ambiguity attacks. Obviously, it is desirable to have an imperceptible, robust, and secure watermarking technique.

Spread spectrum techniques⁶ construct the watermark such that the energy of the watermark at each pixel of the image is low. This allows imperceptible embedding. A strength parameter specifies the amplitude scaling factor of the watermark. The strength may be fixed for the entire image or varied according to a perceptual model.⁷ Cox⁶ suggests inserting the watermark in the most significant coefficients of the image such that attempts to remove the watermark necessitate significant damage to the watermarked image. Another technique⁸ orders the coefficients in a zig-zag scan, skipping the 16000 most significant coefficients and inserting the watermark in the next 25000 coefficients. A common issue of spread spectrum techniques is that the number and locations of the significant coefficients of the watermarking technique that inserts the watermark in the most significant coefficients of blind watermarking technique that inserts the watermark in the most significant coefficients of the image. However, Dugad's technique does not embed the watermark into many coefficients of the image, and is vulnerable to attacks such as sharpening. The technique is also prone to false positives caused by host-signal interference.

In this paper, we describe a new blind watermarking technique for images which is based on Dugad⁹ but inserts the watermark in a different manner. Our method embeds the watermark in the discrete wavelet transform (DWT) domain, where the significant coefficients are determined similarly to the embedded zerotree wavelet¹⁰ (EZW) compression technique. By using EZW concepts, we obtain coefficients that are related to each other by a tree structure. This relationship amongst the wavelet coefficients allows our technique to embed the watermark into more coefficients than Dugad, and also allows the detector to recover synchronization when the locations of the significant coefficients of the watermarked image change from attacks. Our technique produces an image-dependent watermark, which makes forgery and copy attacks¹¹ more challenging.

In addition to the watermark, we insert a template into the watermarked image. The template contains synchronization information, allowing the detector to determine the geometric transformations performed on the watermarked image. Our template consists of a set of peaks inserted into the Discrete Fourier Transform (DFT) of the watermarked image. To detect the template, we use the cross-ratio (CR) of four collinear points. The CR has been used to insert a watermark directly,¹² however this scheme inserts many peaks into the DFT and the detector must perform a search over the considerable number of peak constellations to detect the watermark. The number of peaks in our template is reduced.

The paper is structured as follows: In Section 2, we describe our embedding approach. Section 3 describes the detection method. Experimental results are presented in Section 4, and Section 5 has our conclusions.

2. THE EMBEDDING METHOD

In this section, we describe our embedding approach. First, we describe how the watermark is constructed and inserted into an original image to produce the watermarked image. Second, we describe the visual model. Finally, we describe our synchronization template.

2.1. Watermark Construction

One of the assumptions of the EZW compression technique is that wavelet coefficients across multiple scales are correlated. Specifically, if a wavelet coefficient at a coarse scale is insignificant with respect to a given threshold T_1 , then the wavelet coefficients at a finer scale of the same spatial location and orientation (such as horizontal, vertical, diagonal) are likely to be insignificant with respect to T_1 . In EZW compression, the wavelet coefficients are described using a parent-children relationship, where a wavelet coefficient at the coarse scale is the parent of all the wavelet coefficients of finer scales at the same spatial location and orientation. This concept is shown in Figure 1, where each sub-band of the DWT is identified by a numeral.

The watermark embedder accepts the original image and secret watermark embedding key K_E as inputs, and produces the watermarked image as the output. The watermark construction and embedding procedure is as follows:



Figure 1. Parent-children relationship of wavelet coefficients

- 1. Obtain the DWT of the original image. Our implementation obtains a three level DWT using the biorthogonal (9–7) Daubechies¹³ filters by lifting.¹⁴
- 2. The lowest pass sub-band (sub-band 1 on Fig. 1) is not involved in watermarking. Let $S = \{s_1, s_2, \ldots, s_k, \ldots\}$ be the set of significant coefficients in sub-bands 2, 3, and 4, where a wavelet coefficient is significant if its magnitude is larger than a threshold T_1 . Each significant coefficient is identified as a tuple $s_k = (b_k, x_k, y_k, v_k)$, where b_k is the sub-band (2, 3, or 4), x_k and y_k are the position of the coefficient in the sub-band, and v_k is the value of the coefficient.
- 3. For each $s_k \in \mathcal{S}$:
 - (a) A zero-mean unit variance Gaussian pseudo-random number generator is seeded with

$$seed = f(K_E, b_k, x_k, y_k) \tag{1}$$

where f is a function that depends only on the embedding key and the sub-band and position of s_k .

(b) s_k is watermarked by

$$v_k' = v_k + \alpha_k |v_k| \rho_{k,0} \tag{2}$$

where v'_k is the value of s_k after watermark embedding, α_k is the amplitude scaling factor, and $\rho_{k,0}$ is a value produced by the pseudo-random number generator. The amplitude scaling factor will be discussed in Sec. 2.2.

- (c) Let $\mathcal{C}_k = \{c_{k,1}, c_{k,2}, \ldots, c_{k,i}, \ldots\}$ be the (direct) children of s_k in the wavelet decomposition.
- (d) The children are watermarked:

$$v_{k,i}' = v_{k,i} + \alpha_k |v_{k,i}| \rho_{k,i} \tag{3}$$

where $v'_{k,i}$ is the value of $c_{k,i}$ after watermark embedding, $v_{k,i}$ is the original value of $c_{k,i}$, and $\rho_{k,i}$ is produced by the random number generator.

- (e) If the magnitude of any $c_{k,i}$ is larger than $T_1/2$, then the watermark is embedded in the children of $c_{k,i}$. Steps 3d and 3e are repeated for all the children of $c_{k,i}$, and all their descendants as necessary. The threshold is halved for each sub-band level.
- 4. The inverse DWT is performed to obtain the watermarked image.
- 5. The synchronization template is inserted into the watermarked image for improved robustness against geometric attacks. The synchronization template is inserted in the Discrete Fourier Transform (DFT) domain, and will be discussed in Sec. 2.3.

The embedding procedure embeds the watermark into each of the significant coefficients in the coarsest subbands (the s_k 's) and their significant descendants. The random number generator is seeded prior to watermarking each s_k , which provides robustness against attacks. Consider an attack which manipulates the wavelet coefficients such that some insignificant coefficients in the watermarked image become significant in the attacked image. Similarly, the attack may also cause some significant coefficients in the watermarked image to become insignificant in the attacked image. When the detector examines the attacked image, a different set of significant coefficients will be obtained. If the watermark embedder does not perform step 3a, then the detector is likely to lose synchronization and fail to detect the watermark. This loss of synchronization may occur even if the attack causes a change in a single wavelet coefficient. By re-seeding the random number generator, the detector can re-synchronize at each s_k , even when the number of significant coefficients change in the s_k 's or their descendants.

2.2. Perceptual Model

There has been much work to improve the imperceptibility of the watermark as well as robustness to attacks by using perceptual models. Many perceptual models obtain just-noticeable difference (JND) thresholds, which describe how much each pixel or transform coefficient of an image can be changed without impacting watermark visibility.^{7,15} In this paper, we adopt a simple perceptual model for watermark insertion. Our perceptual model assumes that the watermark may be inserted more strongly on the edges and textured regions of an image than the flat or smooth regions. The DWT provides information about the local activity of an image, because wavelet coefficients with large magnitude are usually related to the presence of edges in the spatial domain.

In our perceptual model, an activity image \mathcal{A} is created having same dimensions as the coarsest sub-band (sub-band 1). Each pixel $a(x, y) \in \mathcal{A}$ has a binary value:

$$a(x,y) = \begin{cases} 1 & \text{if } |v_2(x,y)| > T_1 & \text{or } |v_3(x,y)| > T_1 & \text{or } |v_4(x,y)| > T_1 \\ 0 & \text{otherwise} \end{cases}$$
(4)

where $v_n(x, y)$ is the value of the wavelet coefficient in the (x, y) position of sub-band n. The activity image is used to determine the amplitude scaling factor (a_k) for watermarking s_k in step 3b of the watermark embedding process, as explained below. The same value of α_k is used for watermarking all descendants of s_k in step 3d. Figure 2 shows \mathcal{A} obtained from two example images using the threshold $T_1 = 40$. The boxed areas indicate regions of the image in which the corresponding a(x, y) = 1.

To obtain α_k for coefficient s_k , an $N \ge N$ (such as 3x3 or 5x5) window \mathcal{W} is centered at $a(x_k, y_k)$. Let Z_k be the count of pixels in \mathcal{W} that have the value 1, or

$$Z_k = \sum_{a(x,y)\in\mathcal{W}} a(x,y) \tag{5}$$

The amplitude scaling factor α_k is then obtained by

$$\alpha_k = \begin{cases} \gamma \alpha & \text{if } Z_k = 1 \text{ or } Z_k \ge N^2 - 1 \\ \alpha & \text{otherwise} \end{cases}$$
(6)

where α is the global amplitude scaling factor and $\gamma > 1.0$ is the gain when the visual model decides that an edge or texture is present.



Figure 2. Example activity images. Boxed areas indicate the regions where a(x, y) = 1

2.3. Template Embedding

A challenge in blind watermark detection is that of synchronization, particularly when the watermarked image is subjected to geometric attack and distortion. Geometric attacks include image re-scaling, rotation, warping, and translation (shifting). A geometric attack confuses the watermark detector by transforming the coordinates of the watermark, effectively relocating the watermark embedded in the attacked image. Generally, the watermark will not be detected unless the watermark detector obtains the coordinate transformation applied by the geometric attack. Unfortunately, obtaining the coordinate transformation using blind search is computationally expensive and prone to false positives.¹⁶ To address the vulnerability against geometric attacks, a template is created in the watermarked signal. The template contains synchronization information which allows the detector to efficiently obtain the coordinates of the watermark.

One way to produce a template is to insert a synchronization signal into the watermarked image. The synchronization signal may consist of an arrangement of peaks in the DFT domain¹⁷ or peaks with a defined structure.¹⁸ Our template is based on the previous work,¹⁸ however the peaks in our template are also related by using the cross-ratio of four collinear points (CR).¹² This relation is used to identify peaks of the synchronization template from other peaks in the DFT (such as peaks from the original image), which reduces false positives when the detector performs template matching. The objective of using the CR is to obtain stronger template against attacks and possible false positives.

The CR between four points A, B, C, D located at $(x_a, y_a), \ldots, (x_d, y_d)$ in two-dimensional space is defined as follows:

$$CR = \frac{\overline{AC} \cdot \overline{BD}}{\overline{AD} \cdot \overline{BC}} \tag{7}$$

$$\overline{AC} = \sqrt{(x_a - x_c)^2 + (y_a - y_c)^2}$$
(8)

where A, B, C and D are arranged collinearly in the order A - B - C - D.

Our template consists of two sets of 4 collinear peaks embedded in the DFT domain at angles θ_1 and θ_2 with radii varying between f_{t1} and f_{t2} as shown in Figure 3. We require at least two lines in order to resolve ambiguities arising from the symmetry of the magnitude of the DFT. The CR of the two sets of peaks are χ_1 and χ_2 , which must be provided to the watermark detector as side-information.

 χ_1 and χ_2 are used by the watermark detector to identify the peaks of the template. The cross-ratio of four collinear points (CR) has been adopted because of its resistance against geometrical attacks.¹² The CR is



Figure 3. Template structure

invariant under affine or perspective transformations. Therefore, although the template will be affected in the Fourier domain by a geometric transformation, the CR of its peaks remains unchanged. The strength of the template is determined adaptively as well. We find that inserting each template peak with magnitude equal to the sum of the local average and standard deviation of the DFT magnitudes near where the peak will be inserted provides a good compromise between visibility and robustness during decoding.

3. DETECTION METHOD

Watermark detection is a two-step process. First, the template is detected. Using the template, geometric transformations are "reversed" and then the watermark is detected.

3.1. Template Detection

Our template consists of eight peaks which are arranged in two lines which intersect through the origin. The following steps are performed to detect the template:

- 1. Obtain the DFT of the image. The image is padded to 1024x1024 pixels prior to the DFT.
- 2. Extract the positions of all local maxima (peaks) (p_{xi}, p_{yi}) in the DFT magnitude. One way to identify local maxima is to use a sliding window and compare the DFT magnitude at the center of the window with other DFT magnitudes in the window.
- 3. Search for sets of 4 collinear peaks $\Gamma = \{\mathcal{L}_1, \mathcal{L}_2, \ldots\}, \mathcal{L}_i = (p_{i,1}, p_{i,2}, p_{i,3}, p_{i,4})$ that are arranged to form a line passing through the origin. This search is performed by obtaining the slope between all pairs of peaks and then comparing the slopes for collinearity.
- 4. There will generally be many sets of collinear points in Γ . The cross-ratio of each $\mathcal{L}_i \in \Gamma$ is obtained by (7), and the two sets of four peaks whose CRs are closest to χ_1 and χ_2 are used to estimate the affine transformation in a manner similar in principle to the previous work.¹⁸

3.2. Watermark Detection

The watermark detector is correlation-based, similar to Dugad.⁹ The detector uses a similar procedure to the watermark embedder (Sec. 2.1) to obtain the watermark from the detection key $K_D = K_E$ and from the significant coefficients of the input image, except that significance of wavelet coefficients is determined by comparison with

threshold $T_2 \ge T_1$. T_2 is larger than T_1 to avoid correlating wavelet coefficients that are not watermarked. Once the watermark is obtained, it is correlated with the significant wavelet coefficients of the input image:

$$Z = \frac{1}{M} \sum_{i=1}^{M} \hat{V}_i y_i \tag{9}$$

where \hat{V}_i is the *i*-th wavelet coefficient of the input image, y_i is the value of the *i*-th watermark sample, *i* is an index over all the significant coefficients of the input image and *M* is the number of such coefficients. The detection threshold is identical to Dugad,⁹

$$S = \frac{\alpha}{2M} \sum_{i=1}^{M} |\hat{V}_i| \tag{10}$$

If $Z \geq S$, the watermark is present in the detector input image.

4. EXPERIMENTAL RESULTS

We have implemented our watermarking technique to evaluate the robustness of the watermark under attack. In our implementation, the threshold for significance of wavelet coefficients for the watermark embedder is $T_1 = 40$ and the detector is $T_2 = 50$, which are identical to the thresholds used by Dugad.⁹ The visual model uses $\gamma = 2$. Figure 4 shows the performance of the proposed watermarking technique under various attacks using the *Lena* image. The results are similar for other images that were examined. From Fig. 4(a), we observe that the correlation value Z obtained using $K_D = K_E$ is much larger than the threshold S, and that Z obtained using other detection keys are below the threshold. Fig. 4(b) show the robustness of our watermark against JPEG compression, even for low JPEG quality factors. Fig. 4(c) show that the watermark is successfully detected after 3x3 median filtering, however we note that our algorithm has the same problems with 4x4 median filtering as Dugad.⁹ Fig. 4(d) shows that our technique is robust against FMLR (Frequency Mode Laplacian Removal).¹⁹ Finally, Figs. 5(a) and 5(b) show that the correlation value obtained using our proposed technique is well above the detection threshold for when using the correct K_D , however the correlation value falls below the threshold for Dugad's method.⁹

For our template, we observed that the peak positions are discretized, and thus it may not be possible to obtain four points that are strictly collinear. This causes the template detection to fail. There are two consequences: First, there is some uncertainty in determining whether four points fall in a straight line through the origin in step 3 of template detection. Second, the CR values are changed when the four points are not strictly collinear. These two situations can be overcome by developing a more flexible detection methodology. For example, sets of points may be considered in Γ if they are "almost" collinear. A template detector has been implemented which allows the notion of collinearity to be somewhat relaxed. However, the results after geometric attacks such as cropping, rotation, and scaling have been contradictory. Relaxing the collinearity also causes a dramatic increase in the computational cost of template detection.

Finally, we show the effect of the perceptual model described in Sec. 2.2. Fig. 6 shows the *Lena* image watermarked using the perceptual model. Fig. 6(a) uses $\alpha = 0.2$ and $\gamma = 2$, while Fig. 6(b) uses $\alpha = 0.4$ for watermark embedding throughout the image. By comparing these two images, it is noticed that there are areas where an increase in the amplitude of the inserted watermark produces more visible effects than in others areas. The hair of the *Lena* image is an example of area where the effects of increasing the strength of the watermark are not noticeable, compared to regions such as the shoulder and the hat.

5. CONCLUSIONS

This paper describes a new watermarking technique based on the tree structure of the DWT. The technique uses a perceptual model and synchronization template. Experimental results show that the watermark is robust against some signal processing attacks, such as JPEG compression, median filtering, and sharpening. However, more work is needed for the synchronization template. Preliminary results for the template detection are not conclusive relative to the performance against geometric attacks. We believe that a relationship between the



Figure 4. Robustness of the watermark against attack. Vertical axis is the correlation value, horizontal axis for all graphs except 4(b) correspond to detection using different watermark detection keys (K_D) . The embedding key is $K_E = 50$.



Figure 5. Comparison of the robustness of our proposed technique with Dugad's method⁹ under sharpening



(a) Watermarked using perceptual model



(b) Watermarked without using a perceptual model

Figure 6. Watermarked images showing the reduction of watermark visibility when using the proposed perceptual model

points in a template can improve the performance of the template detection. Finally, the proposed adaptive perceptual method shows a good performance to find the best areas to insert a stronger watermark. A version of this algorithm is available in the Watermark Evaluation Testbed at Purdue University.^{20, 21}

REFERENCES

- A. M. Eskicioglu and E. J. Delp, "An overview of multimedia content protection in consumer electronics devices," Signal Processing: Image Communication, vol. 16, no. 7, pp. 618–699, 2001.
- E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, "Advances in digital video content protection," *Proceedings of the IEEE*, 2004, submitted.
- R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarking for images and video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108–1126, July 1999.
- 4. M. Barni, C. I. Podilchuk, F. Bartolini, and E. J. Delp, "Watermark embedding: Hiding a signal within a cover image," *IEEE Communications Magazine*, vol. 39, no. 8, pp. 102–108, Aug. 2001.
- 5. C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33–46, July 2001.
- I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997.
- R. B. Wolfang, C. I. Podilchuck, and E. J. Delp, "Perceptual watermarks for digital images and video," Proceedings of the IEEE, vol. 87, no. 7, pp. 1108–1126, July 1999.
- A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," *Proceedings of the IEEE International Conference on Image Processing*, vol. 3, 1997, pp. 520–523.
- 9. R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images," *Proceedings of the IEEE International Conference on Image Processing*, Chicago, IL,, Oct. 1998.
- J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3445–3465, Dec. 1993.
- M. Kutter, S. Voloshynovskiy, and A. Herrigel, "The watermark copy attack," Proceedings of the SPIE Security and Watermarking of Multimedia Contents II, vol. 3971, Jan. 2000, pp. 371–380.

- R. Caldelli, M. Barni, F.Bartolini, and A. Piva, "Geometric-invariant robust watermarking through constellation matching in the frequency domain," *Proceedings of the IEEE International Conference on Image Processing*, vol. 2, Sept. 2000, pp. 65–68.
- M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet transform," *IEEE Transactions on Image Processing*, vol. 1, no. 2, pp. 205–220, Apr. 1992.
- M. Rabbani and R. Joshi, "An overview of the JPEG 2000 still image compression standard," Signal Processing: Image Communication, vol. 17, no. 1, pp. 3–48, Jan. 2002.
- A. B. Watson, "DCT quantization matrices visually optimized for individual images," Proceedings of the SPIE Human Vision, Visual Processing, and Digital Display IV, vol. 1913, Feb. 1993, pp. 202–216.
- J. Lichtenauer, I. Setyawan, T. Kalker, and R. Lagendijk, "Exhaustive geometrical search and the false positive watermark detection probability," *Proceedings of the SPIE Security and Watermarking of Multimedia Contents V*, vol. 5020, Santa Clara, CA, Jan. 21–24, 2003, pp. 203–214.
- S. Pereira, J. J. K. O. Ruanaidh, F. Deguillame, G. Csurka, and T. Pun, "Template based recovery of Fourierbased watermarks using log-polar and log-log maps," *Proceedings of the IEEE International Conference on Multimedia Computing Systems, Special Session Multimedia Data Security Watermarking*, June 1999.
- S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Transac*tions on Image Processing, vol. 9, no. 6, pp. 1123–1129, June 2000.
- R. Barnett and D. E. Pearson, "Frequency mode LR attack operator for digitally watermarked images," *Electronics Letters*, vol. 34, no. 19, pp. 1837–1839, Sept. 1998.
- H. C. Kim, H. Ogunleye, O. Guitart, and E. J. Delp, "The watermark evaluation testbed (WET)," Proceedings of the SPIE Security, Steganography, and Watermarking of Multimedia Contents VI, vol. 5306, San Jose, CA, January 19–22, 2004.
- 21. B. Macq, J. Dittmann, and E. J. Delp, "Benchmarking of image watermarking algorithms for digital rights management," *Proceedings of the IEEE*, 2004, to be published.