

March 25, 2001

Professor J Illingworth
Michael Faraday House,
IEE Proceedings
Microwaves, Antennas and Propagation

Dear Editor Illingworth,

Thank you for your letter of February 7, 2000, in which you noticed us that our manuscript entitled "A Robust Digital Signature Scheme for Protecting Images and Graphics Copyrights (Paper No. 23227)" is required revision for publication in **IEE Proceedings Microwaves, Antennas and Propagation**.

The comments of the regarding our manuscript were extremely helpful to us in preparing a clearer version. We have rewritten many paragraphs according to the recommendations of the referees. In addition, the revised paper has been proofread by a good technical writer whose first language is English. Thank you very much for your advisement.

Attached are a copy of the revised version of the manuscript and a list of the revisions. Your acknowledgement will be greatly appreciated. Thank you again.

Sincerely yours,

XXX
Professor
Dept. of yyy
zzz University

Tel:

Fax:

Email:

LIST OF REVISIONS

Author: Chang et al.

Title: A Robust Digital Signature Scheme for Protecting Images and Graphics Copyrights.

Paper Number: 23227

The comments of the reviewers regarding our manuscript were extremely helpful to us in preparing a clearer version. We have revised our manuscript according to the reviewers' suggestions. The major revised parts are briefly described as follows:

(A) Response to the suggestions of Reviewer 1:

1. We inserted many more sources into the reference section for readers who are interested in further study of digital watermarking.
2. The differences between our work and Pitas et al.'s work can be found in the third paragraph of Section 6. We briefly list the difference as follows: a) Our method is suitable for digital cartoons and map graphics. b) The watermark used in our method is a grey level image rather than a binary image. c) Our approach does not embed the watermark into the host images or graphics.
3. We have further explained that $|A|$ denotes the determinant of A in Section 3, Line 3 (Page 8).
4. An really means A^n . In addition, the computation results are the same as in Equation (4) applied n times because there is a modulus N.
5. Yes, we agree that our method is not fully robust to cropping. However, our main purpose is to illustrate that exact spatial coordinates are not required in this case. We have rewritten the sixth paragraph of Section 5 to explain this.

(B) Response to the suggestions of Reviewer 2:

1. We have analyzed the security of the proposed method in the fourth paragraph of Section 6 (Page 14).
2. We have inserted a sentence in Lines 3-4 (Page 5) to emphasize the meaning of "watermark-like". In a nutshell, our method is like traditional watermarking in purpose rather than in methodology. Moreover, the comparisons between traditional watermarking and our scheme have been described in the third

paragraph of Section 6 (Page 14).

3. Yes, we agree with the reviewer's opinion and we have replaced the term "signature" with "authentication" in the proper places throughout this paper. In addition, the title has also been changed to "A Robust Authentication Scheme for Protecting Copyrights of Images and Graphics".
4. We have analyzed the size of the authenticator tag (secret key) in the second paragraph of Section 6 (Page 13).
5. We are in agreement with the reviewer's opinion that the torus automorphism is a convenient and useful two-dimensional permutation function. In addition, we believe that most readers have never heard of it, so we introduce the torus automorphism in this paper for the convenience of the reader. However, according to the suggestion of the reviewer, we have shortened Section 3 and removed two illustrations from that section.

(C) Response to the suggestions of Reviewer 3:

1. We are not sure whether or not our scheme is similar to the checksum of the coding theory. Nevertheless, our scheme takes into consideration the distortion allowable feature of digital images. As the experimental results show, our scheme is robust to resist various attacks.
2. We appreciate very much the reviewer's suggestion and we will consider O'Ruanaidh's RST invariant log-polar mapping in our future work.
3. It is true that recognizing a picture watermark depends upon the viewer as well as the watermark. So a decision by the majority is a natural way to solve this problem. Constructing a formal mechanism to recognize a picture watermark is a good research topic. The mechanism is a useful auxiliary tool. For example, PSNR provides a subjective judgement of a processed image's quality.
4. If random-values are used as a watermark, the PSNR may be smaller than that obtained by using a meaningful image (please refer to our extended method 1, Page 10). In particular, random values are hard to recognize with the human eye. That is why we recommended using the meaningful image as a watermark in the first paragraph of Section 6 (Page 13).
5. Issuing a time-stamp is the main objective of TSS. However, it is a good point that TSS embeds some key information, e.g., dimensions of image/watermark, into the time-stamp. We will further study the ramifications of this discovery in our future work.