International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# Issue of Authorized Electronic Seals Based on the Content of Documents

**Shanjun Zhang [1]* Kazuyoshi Yoshino[2] Hongbing Zhu[3]**

[1] *Dept. information science, Faculty of Science, Kanagawa University*
[2] *Dept. of Welfare Systems Engineering, Kanagawa Institute of Technology*
[3] *Faculty of information design, Hiroshima Kokusai Gakuin University*
* Corresponding author's Email: zhang@info.kanagawa-u.ac.jp

**Abstract:** With the progress of the internet, many import documents can be found online. It is vital to protect the safety and genuineness of the seals in the published documents. In this paper, A fragile watermarking scheme is proposed to extract the features from the original documents and then combine them with some confidential parameters to generate watermarked unique seals from the official seals without affecting the layout and the visible image of the original ones.

**Keywords:** Seal; Watermark; Security; Genuineness

## 1. Introduction

Seal is said to be first used by the Sumerian about 5500 years ago in cuneiform to show the belongings of the merchandise and private property [1]. Then it is found to be used by the ancient Egyptian and Rome. With the influence of China, seal is widely used by Chinese, Korean and Japanese in their daily life in East Asia. The stamp of the Empire's golden seal represents the mighty power of the king. Any attempt to make a fake empire's seal means death in those ages. The golden seal is kept safe under strict surveillance. Official seal of the government represents its authority as well. For ordinary people, seal is necessary for the contracts in economic activities. In many Asian countries, seal is traditionally used to ensure the credibility and authority of the paper documents. Seal is regarded as one of the most important items not only for the governments but also for ordinary people.

Nowadays, with the wide spread of the application and rapid progress of the internet, many public certifications and official documents can be directly found in the interconnected networks, which makes it easy to get the seal image. On the other hand, the promotion of the electronic governments facilitates the access to the seal image. The easy manipulation and transmission of digital media has been a big threat of forgery to the electronic governments' projects. It is very important to protect the safety and genuineness of the officially published documents, especially the genuineness of the official seals. It is vital to ensure that any part of the official seal images which are extracted cut-and-paste from other existing documents are not used elsewhere illegally.

During the last decades, digital watermarking, and more generally, data hiding, has been one of the most active research fields in the signal /image processing area[2][4]. Many technical results have been made all over the world for ownership protection [5]-[10], content authentication [11]-[15], and side information conveyance [16]-[18]. For ownership protection, robustness is one of the major concerns. The watermarks of robust watermarking schemes are expected to survive different types of manipulation to some extent, while the schemes for the purposes of authentication and content integrity verification are supposed to be fragile so that

changes or modifications of a media will be reflected in the hidden watermark. For the purpose of side information conveyance, a watermark is required to convey more information than a robust watermark does. Most of the existing watermarking schemes are designed for either ownership protection or content authentication.

In this paper, we proposed a novel watermarking method to reflect the authentication and protection of the content integrity of the document simultaneously. Our purpose is to provide a means to issue a unique seal image for every particular document. In our proposed method, we guard the seal image rather than the seal itself. The originally stamped seal image is replaced by a watermarked seal image at the same place of the original document before it is circulated publicly in the internet. The watermark is designed according to the content of the original document apart from the original seal image, which is also related to the position of the original seal image in the document. Thus it becomes a secrete key to the owner of the seal. The watermark can then be embedded and detected from the seal image in the document. In this way, if a forged seal image is used in a document by cropping a real seal image from some other documents, a mismatch between the content of the document and the watermark will expose the tampering.

The remainder of this paper is organized as follows. In Section 2, the watermarking scheme explains the generation of the documents with watermark and the watermark embedding/detecting algorithm in detail. In Section 3, some experimental results are given to show the efficiency of our proposal. Conclusion is given in Section 4.

## 2. Proposed watermarking scheme

In this section, we will describe the watermarking scheme in detail. As shown in Fig.1, the host document with original seal image is split into two parts: the seal image part and the remainder image part. After the original seal image is cropped from the original document, the same area of the original seal image is first filled with white blank. Then a sequence of 128 bits of binary watermark is generated according to the content feature of the remainder image, the center position of the original seal image and a secrete bit sequences coded by a secrete key on the dates of sign or stamp. After that the seal image is divided into 8x16 blocks, and each block is embedded with a bit in the watermark according to the even/odd parity of the block.

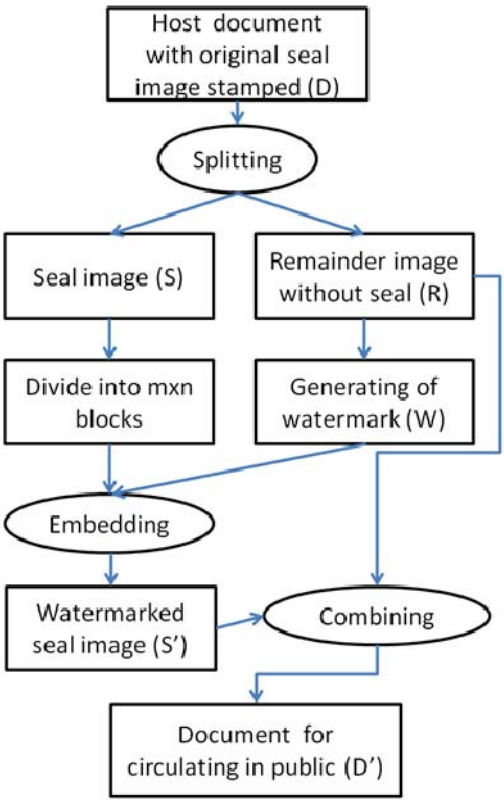



Figure 1 Flowchart of the watermarking scheme

Finally, the watermarked seal image will be combined with the remainder image to replace the original seal image. In this way, the original images of the genuine seal will never be used in public circumstances. Instead, a fragile watermarked seal is made and stamped according to the content of the documents. As a result, we do not have to fear for the forged seal images which are "stolen" through "cut-and-paste" from other existing documents, because every seal image in the publicly circulated documents can be assumed to be unique.

### 2.1. Generation of the watermark sequence

The watermark of the binary sequence consists of 128 bits which are constructed from four parts denoted as W1, W2, W3 and W4 here. W1 is a sequence of 64 bits generated as part of the watermark. W1 is used to reflect the global intensity distribution features of the remainder image (R) of the original document shown in Fig. 1. The remainder image is divided by 8x8 blocks. The average intensity of each block is used as a threshold for the block. If the intensity of the pixel in a block is greater than the average intensity of the block, the pixel is counted as a white pixel, or

else it is counted as a black pixel. After that, the blank ratio of the number of the white pixels to the whole number of the pixels in the block is calculated. If the blank ratio of a block is less than 10%, the block will be ranked as 0, if it is greater than 10% but less than 20%, it will be ranked as 1, and so on. Then the blank ratio of each of the 64 blocks is ranked from 0 to 9 levels. The rank numbers are then compared with 64 pseudo-random numbers which are generated among 0 to 9 by linear congruent method following equation (1). If the rank number of a block is greater than the corresponded pseudo random a bit of "1" will be generated, or else a bit of "0" will be generated.

$$x_{n+1} = (A \times x_n + B) \bmod M \qquad (1)$$

$$q_n = x_n \bmod K$$

$$k = q_n \bmod 3$$

Where, $A, B, M, K$ and $x_0$ are given parameters. By changing the parameters, one can change the pattern of the pseudo random series, and thus change W1 for a particular remainder image (R).

Compared with W1, W2 is used to reflect the subtle changes of the remainder image of the original document. The remainder image is check by an 8x4 block. If the intensity sum of a block is an odd number, '1' will be generated, or else '0' will be generated corresponding to the block. In this way, a series of 32 bits is generated to reflect the subtle changes of the particular areas in the remainder image.

The center coordinates of the seal image in the document may vary for different documents. Suppose the maximum size of the document image is 2048 by 2048, we can use 22 bits to express the x, y coordinates of the central position of the seal in the document. The coordinates of the seal center and W2 and 10 preserved bits can be concated to compose a binary sequence of 64 bits. This binary sequence is denoted W3 here to reflect the subtle features of the original document as shown in table 1. The preserved 10 bits can be used to classify the catalogues of the seals used in the document, or can be used to indicate the importance of the documents or some other special purpose.

W4 is defined by a secrete key. The key is used to encode the dates of the sign or stamp into 64 bits of binary sequence. Then W4 is subjected to an

$$w = \langle w1, w3 \oplus w4 \rangle \qquad (2)$$

EXCLUSIVE-OR (XOR) operation with W3. Finally, W1 is concatenated with the XOR result of W3 and W4 to form the watermark sequence W.

Table1. The contents of W3

| X coordinate | Y coordinate | W2 | preserved |
|---|---|---|---|
| 11 bits | 11 bits | 32 bits | 10 bits |

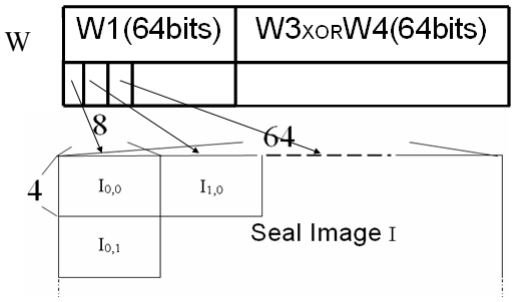



Figure 2. Watermark Q and seal image I

The generation of W is a trade-off among the computation complexity, the length of the watermark, the uniqueness and noise fluctuation of the document, and the content integrity of the document with the seal stamped. The generated scheme is robust enough. Even though the structure and calculation algorithm can be known by others, without knowing the same parameters used in the linear congruent method or the secrete key, same watermark cannot be made from a seal image.

### 2.2. Watermark embedment and authentication

To embed the watermark, the Seal image I is first cropped from the original document as the target image, and then the cropped area of the original document is temporary filled with zero. After that, a binary sequence of the watermark W with a secret key and parameters is generated according to the document image as described in section 2.1. The target image I is divided into 8x16(=128) blocks as shown in Fig.2, where each block is corresponded to a bit of the binary watermark W. For each of the block $I_{ij}$, a bit plane $I_{ij}(k)$ is selected according to a pseudo random

number k. The range of k is from 0 to 3.The parity of the sum of the bit plane $I_{ij}(k)$ is checked to decide how to embed the watermark into the target image. If the parity is odd, and the corresponded bit of Q is 'one', then no change will be made in the bit plane of the target image; if the parity is odd and the watermark bit is 'zero', then one bit of the bit plane will be reversed from 'zero' to 'one', or from 'one' to 'zero'. Similarly, if the parity of the sum of the bit plane of $I_{ij}(k)$ is even and the watermark bit is 'zero', then no change will be made, or a bit will be randomly selected to reverse from 'zero' to 'one', or from 'one' to 'zero'. After all the blocks are processed, the result will be inserted into the original document to replace the area which is temporarily set to be zero.

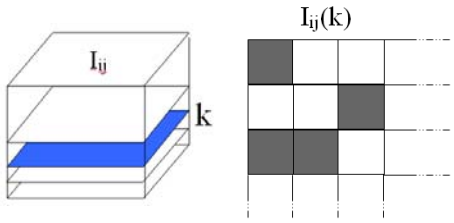



Figure 3. Bit plane randomly selected from target image block $I_{ij}(k)$

Now, the watermark embedding algorithm can be described as follows:

Step1. Extract the original seal image I from the host document.

Step2. Fill the extracted area with white for the remainder image.

Step3. Generate W1, W2, W3 from the remainder image.

Step4. Generate W4 with a secret key on the date.

Step5. Generate the binary watermark W according to formula (2).

Step6. Divide the original seal image into 8x16 blocks.

Step7. For each block I(i,j), select a bit plane k according to a predefined pseudo random number, calculate the sum S of the bits in k plane of block I(i,j).

Step 7.1 IF (Parity(S) == even && W(i+j*8)== 1) do nothing,;

Step 7.2 IF (Parity(S) == odd && W(i+j*8) == 0) do nothing;;

Step 7.3 Select another bit from the bit plane k and change it from 0 to 1, or from 1 to 0 (the bit is randomly selected in the bit plane);

Step 7.4 Do Step 7. for the next block to embed the next bit in the watermark.

Step8. Paste watermarked seal image back to the host document.

In the above algorithm, according to the content of the watermark, only about half of the blocks of the original seal image may need to change a bit in the lower bit plane on the average. As the bit is randomly selected in the block, the differences before and after the embedding process will not be noticed. And the watermarked seal image J will be put to the same position of the original seal image.

For the verifier, the seal image J will be automatically cropped out from the document by a predefined size and a pattern matching. Then a binary sequence of watermark W' will be detected from J, and a genuine watermark W will be generated according to the remainder of the document. The consistency of the information W and W' is then checked. If W and W' is completely the same, then the seal image is regarded as the genuine one, otherwise the seal image is regarded as the illegal forgery.

To detect the watermark from image J, the same pseudo random series is used to select a bit plane k of the block. It is marked as Jij(k) for the (i,j) block. Then the parity of the sum of bit plane Jij(k) will be checked to extract the watermark embedded. If the parity is even, a 'one' bit will be extracted, or else a 'zero' bit will be extracted from the block. The secrete information can be recovered from the extracted binary sequence of the watermark.

The extraction and authentication algorithm can be described as follow:

Step1: Find out the center of the seal image through pattern matching, and then extract it from the document with a predefined size.

Step2: Fill the remainder area with white and generate a genuine watermark W in the same way used in embedding algorithm.

Step3: Divide the seal image J into 8x16 blocks.

Step4: For each of the block J(i,j), select a bit plane k by the same pseudo random series according to formula (1), then calculate the sum S of the bits in the bit plane k .

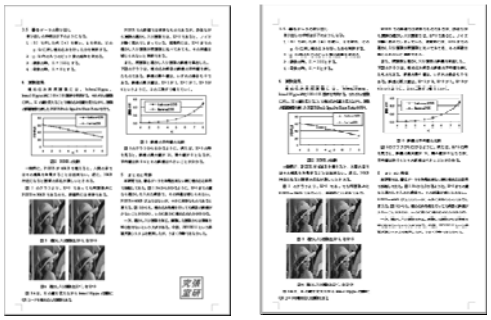
Step4.1: IF (Parity(S) == even) then W'(i+j*8) = 1;

Step4.2: IF(Parity(S) == odd) then W'(i+j*8) = 0;

Step5: Compare W and W', IF (W == W') then the seal is true, otherwise the seal in the document is a forgery.

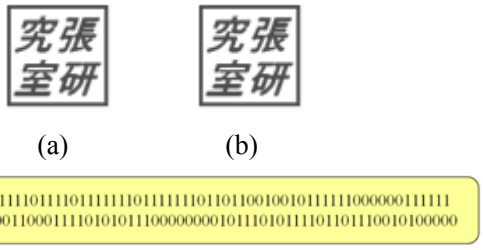
## 3. Experiments

In this section, we show some experimental results. In the following experiments, a set of document images with the size of 494x696 are used. The seal images with the size of 64x64 are replaced with the watermarked ones according to the content of the original documents. Fig.4 (a) shows the original document image; Fig.4 (b) shows the remainder of the document with the seal image cropped. Fig.5 (a) shows the original seal image cropped from Fig.4 (a); Fig.5 (b) shows the watermarked image of the original seal image; Fig.5(c) shows the binary sequence of the



(a) (b)

Figure 4. Original document. (a) Original document with seal image stamped, (b) Original document with seal image cropped.



(a) (b)

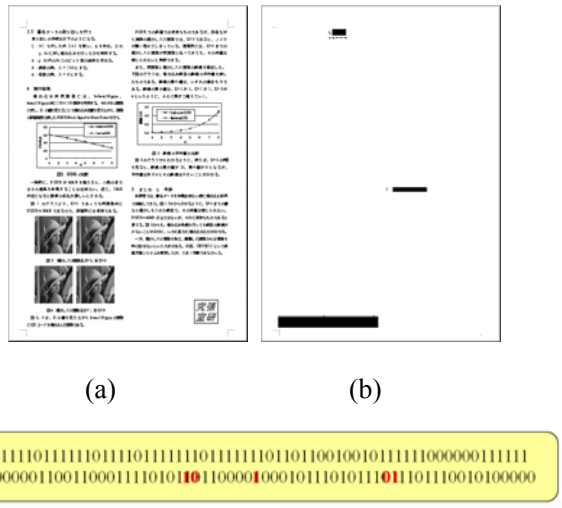
(c)

Figure 5. Seal images. (a) Original seal image cropped from Fig.3., (b) watermarked seal image , (c) binary sequence of the watermark generated from

watermark generated from the document image of Fig.4 (b) where the seal image area is replaced by a blank. The differences of the appearances of Fig.5 (a) and (b) are completely invisible by human eyes. Fig.6 (a) shows a tampered document image of Fig. 4(a) with a completely same seal image stamped at the same position. Fig. 6(b) shows the differences of image Fig.6 (a) and Fig.4 (a). Fig.6 (c) shows the watermark generated from Fig. 6(a) without the seal image. The watermark is different with the watermark detected from the seal image as shown in Fig.5 (c). This reflects that some local minor changes have been introduced into the original document of Fig. 4(a). Some other experiments are shown in Fig.7 with changes in the layout, format, and the position of the seal in the image.Fig.7 (a) shows the original image, 7(b) shows the subtle change in the graph, 7(c) shows the completely same document, only with the different location of the seal. 7(d) shows the same document with different layout. All the changes will result in different watermarks generated from the remainder images and these watermarks will be different from the watermark detected from the cropped seal image.The inconsistency of the watermark will disclose the tamper made in the documents. The watermarks and the differences from the original one are shown in Fig.8.

## 4. Conclusions

In this paper, we have provided a watermarking scheme for seal image authentication based on the content of the original document. A unique watermark is automatically generated according to the intensity distribution of the image or the original

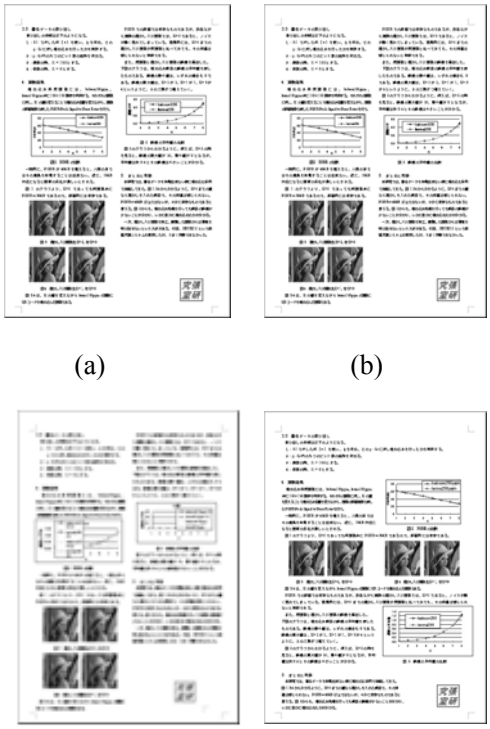


(a) (b)

(c)

Figure 6 (a) The tampered document image, (b) Areas where some characters are changed. (c) The watermark generated from Fig.6(a) without seal image.

document. It is also depended on the parity variation of the logically divided blocks of the original documents, and an encrypted code of the date of the stamp or the date of the creation time.The consistency of the watermark generated by the original document and the one detected from the seal image is checked to decide the authenticity of the seal image without knowing the original genuine one. This is very important because once the real

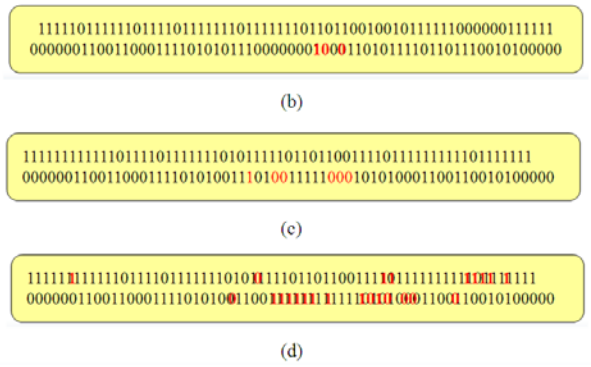


(a) (b)

(c) (d)

Figure 7. Experiments with other changes. (a) Original image. (b)Image with a change in graph (c) Image with a change in the position of the seal. (d) Image with a deferent layout.

seal image is leaked out it can be used for any purpose.To meet this requirement, we select a fragile watermarking method to embed and extract the hidden information. The parity of the sum of the bit plane is critical to the change of the checked block. Without knowing the predefined parameters, no one can properly embed/extract the watermark. However, if the parameters for the pseudo random numbers and the secrete key to the encryption of the date are opened, anybody can check the genuineness of the seal image. With the disclosed parameters, one can extract the watermark embedded in the seal image, but he still cannot recover the original seal image with the watermarked seal image and the watermark, because every bit of the watermark is corresponded to a block, and the changed bit of the bit plane of the block is randomly selected in the block. Experiments have shown the efficiency of the method proposed in the paper. The weak point of our method is that the watermarked seal image is critical to the noise. If noise is introduce into the watermarked bit planes, which make it difficult to extract the watermark properly. In our future work, we are planning to enhance the robustness of the watermark, while remain it fragile to the change of the original document.



(b)

(c)

(d)

Figure 8 (b) Watermark generated from fig.7(b), (c) watermark generated from 7(c). (d) watermark generated from Fig.7(d)

## References


[1] Dominique Colon: 'First Impressions: Cylinder Seals in the Ancient Near East" *Univ of Chicago Pr, 1994.*

[2] Yeung, M.M.: 'Digital watermarking', *Cummun. ACM,* 1998, 41, (7), pp. 30-33

[3] F.A.P., Anderson, R.J., and Kuhn, M.G.: 'Information hiding - a survev', *Proc. IEEE.* 1999. 87. (7). up. 1062-1078

[4] Hartung, F., and Kutter, M.: 'Multimedia watermarking techniques, *Proc. IEEE,* 1999, 87, (7), pp. 1079-1107

[5]I.J.Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing, vol. 6, pp. 1673–1687, Dec. 1997.*

[6] Zhu, B., Swanson, M.D., and Tewfik, A.: 'Transparent robust authentication and distortion measurement technique for images'. *Proc. 7th IEEE Digital Signal Processing Workshop,* Loen, Norway, Sept. 1996, pp. 45–48

[7] Wu, C.-F., and Hseih, W.-S.: 'Image refining using digital watermarking' ,*IEEE Trans. Consum. Electron.,* 2000, 46, (1), pp. 1–5

[8] Kundur, D., and Hatzinakos, D.: 'Diversity and attack characterisation for improved robust watermarking', *IEEE Trans. Signal Process.,* 2001, 49, (10), pp. 2383–2396

[9]C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Trans. Multimedia,* vol. 2, pp. 209–224, Dec. 2000.

[10] Knowles, H.D., Winne, D.A., Canagarajah, C.N., and Bull, D.R.:'A Bayesian approach to attack

characterisation using robust watermarks',*Proc. SPIE–Int. Soc. Opt. Eng.,* 2003, 5150, pp. 851–861

[11] Winne, D.A., Knoweles, H.D., Bull, D.R., and Canagarajah, C.N.:'Digital watermarking in wavelet domain with predistortion for authenticaticity verification and localization', *Proc. SPIE–Int. Soc. Opt. Eng.,* 2002, 4675, pp. 349–356

[12] Wong, P.W., and Memon, N.: 'Secret and public key authentication watermarking schemes that resist vector quantization attack', *Proc. SPIE–Int. Soc. Opt. Eng.,* 2000, 3971

[13] Wu, M., and Liu, B.: 'Watermarking for image authentication'. *Proc. IEEE Int. Conf. on Image Processing,* Chicago, IL, USA, October 1998, Vol. 2, pp. 437–441

[14]D. Kundur and D. Hatzinakos,"Digital watermarking for telltale tamper proofing and authentication," *Proc. IEEE,* vol. 87, pp. 1167–1180, 1999.

[15]C.-Y. Lin and S.-F. Chang, "A robust image authentication method surviving JPEG lossy compression," *Proc. SPIE,* Vol. 3312, 1998.

[16]G. L. Friedman, "The trustworthy digital camera: restoring credibility to the photographic image," *IEEE Trans. Consum. Electron.*, Vol. 39, pp.905–910, 1993.

[17]D. Mukherjee, J. J. Chae, S. K. Mitra, and B. S. Manjunath, "A source and channel-coding framework for video-based data hiding in video," *IEEE Trans. Circuits Syst. Video Technol.,* Vol. 10, pp. 630–645, 2000.

[18] Wolfgang, R.B., Podilchun, C.I., and Delp, E.J.: 'Perceptual watermarks for digital images and video', *Proc. IEEE,* 1999, 87 (7), pp. 1108-1 126