International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015) pp 38468-38469
© Research India Publications. http://www.ripublication.com

Digital Watermarking : Framework for Mathematical Modeling

W. A. W. Adnan[1,2], R. T. Mohamad[3], S.A. Kareem[4], A. A. Zulkefle[3], M.T. Salahudin[5], M. Kamalrudin[6]
[1]Department of Computer and Communication Engineering, Universiti Putra Malaysia, 43400 UPM-Serdang MALAYSIA
[2]King Abdulaziz University, Abdullah Suleiman Street, Al Jamiaa District, 80200, Saudi Arabia
[3]Faculty of Electrical Engineering, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
[4]Faculty of Computer Science & Information Technology, University of Malaya, 50603 Lembah Pantai, Kuala Lumpur, Malaysia.
[5]Centre of Languages and Human Development, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
[6]Faculty of Information & Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
Corresponding author: mohamadrom@utem.edu.my

Abstract- There are three types of watermark extraction methods, namely blind, semi-blind and non-blind. Extraction without reference to the original, un-watermarked, image host is called as blind watermark extraction while extraction methods that rely on some data or features are named semi-blind. Non-blind watermark extraction is the one which needs the original host image for extraction. The watermarking system analyzes the extracted data by evaluating the similarity between the original watermark(*W*) and the extracted watermark(*W'*) during this final stage.

Keywords: Digital Watermaking, Extraction, Image.

Introduction

Watermarking is the process of embedding data called a watermark or tag or label into a multimedia object such that it can be detected or extracted later to make an assertion about the object. All watermarking methods share the same building blocks: an embedding system and the watermark extraction or recovery system (Fridrich 1998a; Hartung & Kutter 1999).The successive stages of watermarking process which comprises of the embedding, the distribution, the extraction and finally the decision (Meerwald 2001). In this embedding stage, an original image (*I*) to be watermarked is pre-processed before embedding a watermark (*W*). In the case of embedding in the transform domain, this may involve converting the image to the desired domain such as the Discrete Cosine Transform (DCT), the Discrete Fourier transform (DFT) and the Wavelet Transform (WT) domains. The watermarked image obtained is then distributed through a digital channel – for example published on a web server or sold to a customer. In the process of transmission and distribution of the watermarked image, compression and other common image processing tasks, may inevitably introduce errors to the watermarked image. All these manipulations on the watermarked image have to be seen as an attack on the embedded information. During this stage the embedded watermark will be extracted. There are three types of watermark extraction methods, namely blind, semi-blind and non-blind. Extraction without reference to the original, un-watermarked, image host is called as blind watermark extraction [Eugene et al, 2007], while extraction methods that rely on some data or features are named semi-blind (Chin-Chen et al, 2007b). Non-blind watermark extraction is the one which needs the original host image for extraction (Zaboli & Moin 2007). The watermarking system analyses the extracted data by evaluating the similarity between the original watermark (*W*) and the extracted watermark (*W'*) during this final stage.

Mathematical Model

The watermark to be embedded, as in Figure 1, may be a binary image, a bit stream or a pseudo-random number that adheres to a desired distribution such as the Gaussian distribution. The watermark(*W*) is then appended to the desired coefficients as shown in Fig. 1 of the transform. The watermarked image(*I'*) is the output of this process such that it is perceptually identical to I and is obtained by performing an inverse transform on the altered transform coefficients. Mathematically, this can be written as

$$E\ (I,K,W) = I' \qquad (1)$$

where *E* is an encoder function and *K* is the secret key.

A decoder function(D) takes a watermarked image(I') whose ownership is to be determined and extracts a watermark(W') from the image using the secret key(K). Mathematically, this is written as

$$D\ (I',I,K) = W' \qquad (2)$$

The extracted watermark(W') will be used in the decision making stage.

The correlation between the recovered information and the original watermark information is used as the similiarity measure(Langelaar, 2000, Mabtoul et al., 2006), defined as

$$Correlation = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j)W^{'}(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}[W(i,j)]^{2}} \quad (3)$$

The value of the correlation determines how closely the original watermark resembles the extracted watermark. If they are identical, then the correlation is equal to 1 (Langelaar, 2000, Mabtoul et al., 2006).

Discussion of Results

The watermarked image(I') is the output of this process such that it is perceptually identical to I and is obtained by performing an inverse transform on the altered transform coefficients. The value of the correlation determines how closely the original watermark resembles the extracted watermark. If they are identical, then the correlation is equal to 1 (Langelaar, 2000, Mabtoul et al., 2006). The correlation between the recovered information and the original watermark information is used as the similiarity measure.

Conclusion

The watermark to be embedded may be a binary image, a bit stream or a pseudo-random number that adheres to a desired distribution such as the Gaussian distribution. The watermarked image(I') is the output of this process such that it is perceptually identical to I and is obtained by performing an inverse transform on the altered transform coefficients which can be expressed mathematically. This can lead to further work in this area of digital watermarking.

References

[1] Fridrich. J., 1998. Image watermarking for tamper detection. *International Conference on Image Processing Proceedings (ICIP 98)*, 2 , p.404 -408.

[2] Hartung. F. & Kutter. M., 1999. Multimedia watermarking technique', *Proceedings of IEEE*, 87, p.1079–1107.

[3] Meerwald. P., 2001. Digital Image Watermarking in the Wavelet Transform Domain. Master's Thesis http://www.cosy.sbg.ac.at/pmeerw/watermarking.

[4] Chin-Chen.C., Chia. C.L., Yih. S.H., 2007. An SVD Oriented Watermark Embedding Scheme with High Qualities for the Restored Images. International Journal of Innovative Computing, Information and Control (IJICIC), 3(3), p.609-620.

[5] Zaboli., S. Moin., M.S., 2007. Non-Blind Adaptive Image Watermarking Approach Based on Entropy in Contourlet Domain. International Symposium on IEEE Industrial Electronics, ISIE 2007. p. 1687-1692.

[6] Langelaar. G., Setyawan. I., Lagendijk. R.L., 2000. Watermarking Digital Image and Video Data- A State-of-the-Art Overview. *IEEE Signal Processing Magazine*, 8-11 September, 17, p.20-43.

[7] Mabtoul. S., Ibn-Elhaj. E., Aboutajdine., 2006. A Blind Chaos-Based Complex Wavelet-Domain Image watermarking Technique *International Journal Computer Science and Network Security*, 6(3), p.134-139.

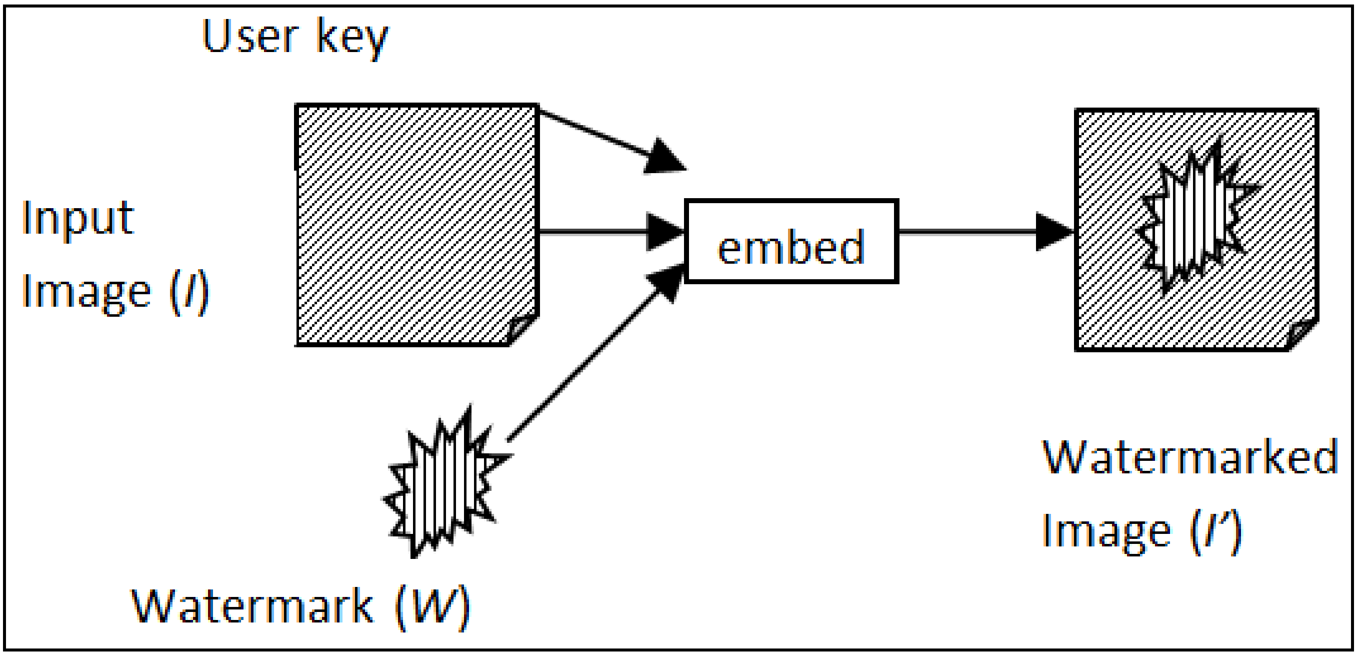

Fig.1. Embedding process