Classification of Watermarking Based upon Various Parameters

Gaurav Chawla
GITM Group of Institutions
Bilaspur, Gurgaon,
Haryana

Ravi Saini
C.M.R.A, GP,Sanghi,
(Rohtak)

Rajkumar Yadav
U.I.E.T, Maharshi Dayanand
University, Rohtak-124001,
Haryana

Kamaldeep
U.I.E.T, Maharshi Dayanand
University, Rohtak-124001,
Haryana

ABSTRACT

With the rapid growth of the Internet and multimedia systems in distributed environments, it is easier for digital data owners to transfer multimedia documents across the Internet. Therefore, there is an increase in concern over copyright protection of digital contents [Piva et al (2002); Lu et al (2001); Lu et al (2000); Lee and Jung (2001)]. Traditionally, encryption and control access techniques were employed to protect the ownership of media. These techniques, however, do not protect against unauthorized copying after the media have been successfully transmitted and decrypted. Recently, watermark techniques are utilized to maintain the copyright [Barni et al (2000); Petitcolas (1999); Eskicioglu and Delp (2001)].In this paper, we study the different types of watermarking based upon the various parameters.

Keywords

Digital Watermarking, Image, Robust etc.

1. INTRODUCTION

Digital watermarking came to be in great demand when sharing information on the Internet became a usual practice. Sharing files online, you never know if someone uses them without your consent. To prevent unauthorized commerce use of your files, you can publish them to the web in the worst quality or don't publish anything worthwhile at all. It isn't a good way to solve the problem of unauthorized use, is it? So, you should look for more effective ways of copyright protection, such as digital watermarking.

A digital watermark is a pattern of bits inserted into a digital file - image, audio or video. Such messages usually carry copyright information of the file. Digital watermarking takes its name from watermarking of paper or money. But the main difference between them is that digital watermarks are supposed to be invisible or at least not changing the perception of original file, unlike paper watermarks, which are supposed to be somewhat visible.

2. TYPES OF WATERMARK

2.1 DIVISION BASED ON HUMAN PERCEPTION

This is sub-divided into visible watermarks and invisible watermarks.

2.1.1 VISIBLE WATERMARKS

These watermarks can be seen clearly by the viewer and can also identify the logo or the owner. Visible watermarking technique changes the original signal. The watermarked signal is different from the original signal [http://en.wikipedia.org/wiki]. (See Figure 2.1)

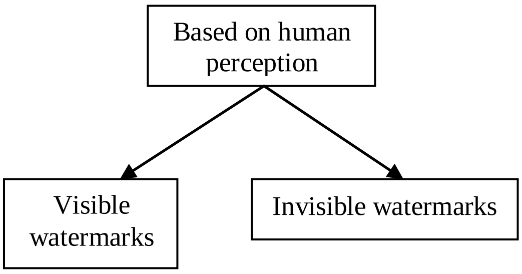

Fig. 2.1 Classification of Watermarks – **Type I**

Visible watermark embedding algorithms are less computationally complex. The watermarked image cannot with stand the signal processing attacks, like the watermark can be cropped from the watermarked image [Latha et al (2007)]. Figure 2.2 shows visible watermarked image.

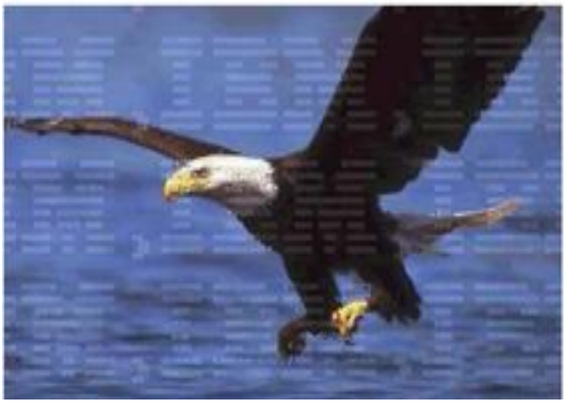

Fig. 2.2 Visible Watermarked Image [Hartung and Kutter (1999)]

Spreading the watermark throughout the image is a best option, but the quality of the image is degraded which prevents the image from being used in medical applications.

2.1.2 INVISIBLE WATERMARKS

These watermarks cannot be seen by the viewer. The output signal does not change much when compared to the original signal. Figure 2.3 shows invisible watermarked image.

Fig. 2.3 Invisible Watermarked Image [Hartung and Kutter (1999)]

The watermarked signal is almost similar to the original signal [http://en.wikipedia.org/wiki]. As the watermark is invisible, the imposter cannot crop the watermark as in visible watermarking.

Invisible watermarking is more robust to signal processing attacks when compared to visible watermarking. As the quality of the image does not suffer much, it can be used in almost all the applications [Latha et al (2007)].

2.2 DIVISION BASED ON APPLICATIONS

Based on application watermarks are sub-divided into fragile, semi-fragile and robust watermarks. (See figure 2.4).

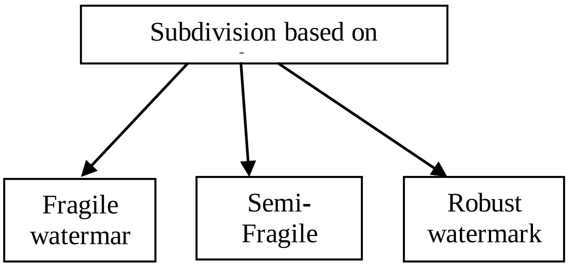

Fig. 2.4 Classification of Watermarks –

2.2.1 FRAGILE WATERMARKS

These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked signal which is shown in figure 2.5.

2.1.2 INVISIBLE WATERMARKS

These watermarks cannot be seen by the viewer. The output signal does not change much when compared to the original signal. Figure 2.3 shows invisible watermarked image.

Fig. 2.3 Invisible Watermarked Image [Hartung & Kutter]

The watermarked signal is almost similar to the original signal [http://en.wikipedia.org/wiki]. As the watermark is invisible, the imposter cannot crop the watermark as in visible watermarking.

Invisible watermarking is more robust to signal processing attacks when compared to visible watermarking. As the quality of the image does not suffer much, it can be used in almost all the applications [Latha et al (2007)].

2.2 DIVISION BASED ON APPLICATIONS

Based on application watermarks are sub-divided into fragile, semi-fragile and robust watermarks. (See figure 2.4).

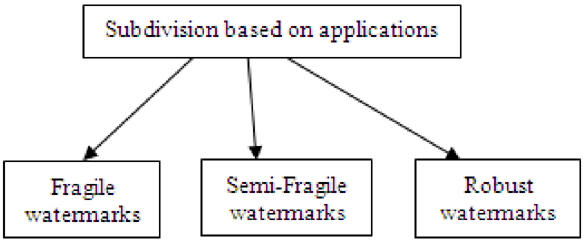

Fig. 2.4 Classification of Watermarks – Type II

2.2.1 FRAGILE WATERMARKS

These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked signal which is shown in figure 2.5.

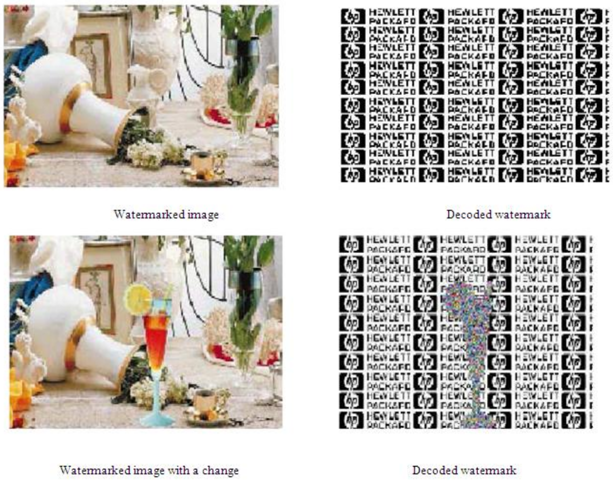

Fig. 2.5 Fragile Watermarked Images

2.2.2 SEMI-FRAGILE WATERMARKS

These watermarks are broken if the modifications to the watermarked signal exceed a pre-defined user threshold. If the threshold is set to zero, then it operates as a fragile watermark. This method can be used to ensure data integrity and also data authentication [Bender et al (1996)].

2.2.3 ROBUST WATERMARKS

These watermarks cannot be broken easily as they withstand many signal processing attacks. Robust watermark should remain intact permanently in the embedded signal such that attempts to remove or destroy the robust watermark will degrade or even may destroy the quality of the image. This method can be used to ensure copyright protection of the signal [Bender et al (1996)].

2.3 Division Based On Level Of Information Required To Detect The Embedded Data [Kejariwal (2003)]

Based on the level of required information all watermarks are sub-divided into blind watermarks, semi-blind watermarks and non-blind watermarks. Figure 2.6 shows the classification of watermarks based on the level of information required to detect the embedded data.

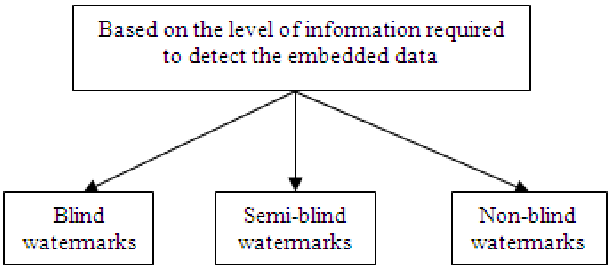
Based on the level of information required to detect the embedded data
Blind watermarks
Semi-blind watermarks
Non-blind watermarks

Fig. 2.6 Classification of Watermarks-Type III

2.3.1 BLIND WATERMARKS

These watermarks detect the embedded information without the use of original signal. They are less robust to any attacks on the signal.

2.3.2 SEMI-BLIND WATERMARKS

These watermarks require some special information to detect the embedded data in the watermarked signal.

2.3.3 NON-BLIND WATERMARKS

These watermarks require the original signal to detect the embedded information in the watermarked signal. They are more robust to any attacks on the signal when compared to blind watermarks.

2.4 Based On User's Authorization To Detect The Watermark [Kejariwal (2003)]

This is sub-divided into public watermarks and private watermarks. Figure 2.7 shows the classification of watermarks based on user's authorization to detect the watermark.

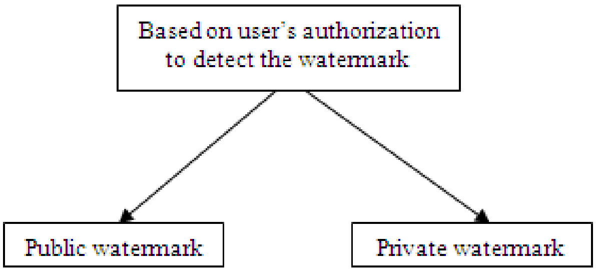

Fig. 2.7 Classification of Watermarks – Type IV

2.4.1 PUBLIC WATERMARKS

In this watermarking, the user is authorized to detect the watermark embedded in the original signal.

2.4.2 PRIVATE WATERMARKS

In this watermarking, the user is not authorized to detect the watermark embedded in the original signal.

2.5 DIVISION BASED ON KNOWLEDGE OF THE USER ON THE PRESENCE OF THE WATERMARK [Kejariwal (2003)]

This is sub-divided into steganographic watermarking and non-steganographic watermarking. (See figure 2.8).

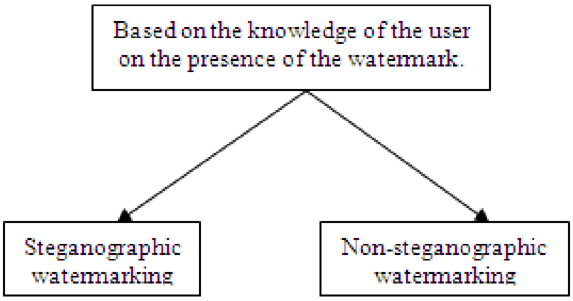
Based on the knowledge of the user on the presence of the watermark.
Steganographic watermarking
Non-steganographic watermarking

Fig. 2.8 Classification of Watermarks – Type V

2.5.1 Steganographic Watermarking

The user is not aware of the presence of the watermark.

2.5.2 Non-Steganographic Watermarking

The user is aware of the presence of the watermark

3. CONCLUSION

In this paper, we studied the various types of watermarking techniques on the basis of various parameters like Human Perception, Robustness etc. On the basis of human perception, we can divide the watermarking into two parts: Visible and Non Visible Watermarking. Based upon the user authorization for the detection of the watermark, watermarking can be divided into public and private watermarking. On the basis of various applications, watermarking can be divided into three categories: Fragile Watermarking, Non-Fragile Watermarking and Robust Watermarking. In the future, we will try to develop some new watermarking techniques which are robust and can be used in various real life applications .

4. REFERENCES

[1] Piva, A., Bartolini, F. and Barni (2002), M., “Managing copyright in open networks”, IEEE Transactions on Internet Computing, Vol. 6, Issue. 3, pp. 18-26.

[2] Lu, C., Huang, S., Sze, C. and Liao, H.Y.M (2000), “Cocktail watermarking for digital image protection”, IEEE Transactions on Multimedia, Vol. 2, pp. 209-224.

[3] Lu, C., Yuan, H. and Liao, M. (2001), “Multipurpose Watermarking for Image Authentication and Protection”, IEEE Transactions on Image Processing, Vol. 10, Issue. 10, pp. 1579-1592.

[4] Lee, J. and Jung, S. (2001), “A survey of watermarking techniques applied to multimedia”, Proceedings IEEE International Symposium on Industrial Electronics (ISIE), Vol. 1, pp. 272-277.

[5] Barni, M., Bartolini, F., Caldelli, R., De Rosa, A. and Piva, A. (2000), “A Robust Watermarking Approach for Raw Video”, Proceedings 10th International Packet Video Workshop, Cagliari, Italy.

[6] Petitcolas, F. (1999), “Information hiding techniques for steganography and digital watermarking Stefan Katzenbeisser”, Artech House Books, ISBN 1-58053-035-4.

[7] Eskicioglu, A. and Delp, E. (2001), “An overview of multimedia content protection in consumer electronics devices”, Proceedings Signal Processing Image Communication, pp. 681-699.

[8] [http://bytescout.com/products/enduser/watermarking/digital_watermark_types.html]

[9] Latha, M.M., Pillai, G.K. and Sheela, K.A. (2007), “Watermarking based content Security and Multimedia Indexing in digital Libraries”, International Conference on Semantic Web and Digital Libraries (ICSD). ARD Prasad & D. P. Madalli (Eds.).

[10] Bender, W. and Gruhl, D. (1996), “Techniques for data hiding”, Ibm Systems Journal, Vol 35, Nos 3&4.

[11] Bender, W., Gruhi, D., Morimota, N. and Lu, A. (1996), “Techniques for Data Hiding”, IBM Systems Journal, Vol. 35, No. 3 & 4.

[12] Hartung, F. and Kutter, M. (1999), “Multimedia Watermarking Techniques”, Proceedings on IEEE, Vol. 87, No. 7, pp: 1079 – 1107.