Research Journal of Applied Sciences, Engineering and Technology 4(14): 2251-2254, 2012
ISSN: 2040-7467

Submitted: March 15, 2012 Accepted: March 26, 2012 Published: July 15, 2012

Image Watermarking Techniques - A Review

S. Priya, B. Santhi and P. Swaminathan
School of Computing, SASTRA University, Thanjavur, 613401, India

Abstract: Multimedia communication technology has developed very rapidly during the last few years. The main aim of the watermarking technique is to protect the confidentiality, integrity, availability and authenticity of information in communication from unauthorized access, reveal, disruption, change and copy. In watermarking the required information is inserted in multimedia data. This study analyzes watermarking techniques, various categories of watermarking and its requirements. This study mainly concentrates on two broad categories of Image watermarking.

Key words: Human visual system, image watermarking techniques, visible and invisible watermarking

INTRODUCTION

In olden days, encoding and control access techniques were used to protect the ownership of media. In order to perform digital signature, multimedia copy right and tamper proof data, the related information should be protected. To protect the information, watermarking is one of the best techniques in this real world.

Watermarking has discovered a lot of explore interest recently. Image watermarking process is described in Fig.1. It is a process of embedding/ inserting/hiding essential image in an image media in a secure manner. The image to be hidden is called as watermark image and the image which carries the watermark image is called as host image or original image or carrier image. Watermarked image is the combination of watermark and host image which is the outcome of watermarking process.

The requirements of watermarking process are listed below:

- **Transparency or fidelity:** The watermarking process should not affect the quality of original and watermark image.
- **Robustness:** The watermarking system should be strong enough to withstand the efforts of watermarking attacks.
- **Imperceptible:** The watermarking process should be imperceptible to the unauthorized user.

Watermark is classified into several categories based on human perception, resistance to attack, image recovery and embedding domain. The water mark classification is shown in Fig. 2. Different watermarking techniques are used in copyright protection, digital signature, tamper proofing, data monitoring and data authentication.

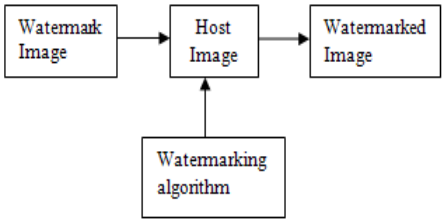

Fig. 1: Watermarking process

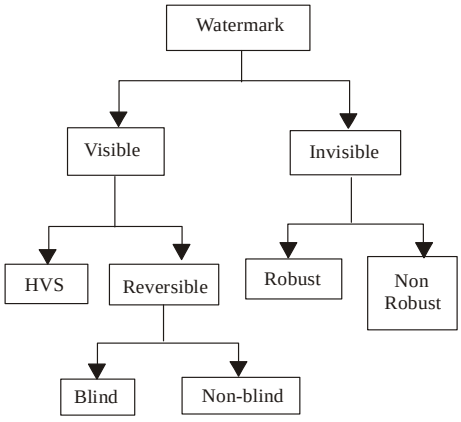

Fig. 2: Watermarking classification

This study is mainly used to analyze various watermarking techniques based on human perception. Based on human view perception the watermarking system is classified into two main categories namely visible and invisible. In visible watermarking the watermark image is visibly embedded over a host image and viewed by the human. In invisible watermarking the watermark image is hidden within a host image. Hence the watermark image cannot be viewed by the human.

Corresponding Author: S. Priya, School of Computing, SASTRA University, Thanjavur, 613401, India

VISIBLE WATERMARKING

A visible watermarking is a process of translucently embedding watermark (logo) image on the primary image/host image. For this watermarking the bit rate and signal strength is high. In this study visible watermarking is classified into two categories namely human visual system and reversible visible watermarking .

Human Visual System (HVS): Watermarking process considers contrast sensitivity model of the human visual systems. The following techniques belong to HVS visible watermarking .

Biao-Bing and Shao-Xian (2006), develop a compound coefficients of host and watermark image is computed using its local and global characteristics. Using Contrast sensitivity function and Discrete Wavelet Transform (DWT) domain, the host and watermark image are split into more blocks. Blocks are classified based on image dimensions (plane, edge and texture). Spatial sensitivity of human varies with respect to the image watermark intensity.

Ying *et al*. (2009), propose an invertible recovery of original image without any watermarking detail at the receiver side. Depending on the scaling factors of HVS the watermarking process is performed by adjusting the pixel value. Based on the difference of image between host image and its approximate version (prediction technique) a reconstruction packet is created for reversibility. HVS characteristics are considered to calculate the greater scale factor and lower scale factor. Then greater and lower scale factors are assigned to mid-luminance and textured areas respectively.

Min-Jen (2009), develops a watermarking technique using DWT. In DWT domain, original and watermark image utilizes local and global characteristics. It is used to find out the best watermarking position and strength at the watermark embedding stage. One-to-one pixel mapping exists between watermark and host image. Watermark pixel is divided into two categories depending on their brightness.

Reversible visible watermarking: Reversible visible watermarking is a process of embedding visible watermark image in the host image and extract the watermark image without any loss. It provides the capability to retain the original image. This type of watermarking is also called as invertible or lossless recovery watermarking . Based on recovery requirements, again it is classified into two types as blind and non-blind watermarking .

Blind reversible visible watermarking: In blind watermarking , the cover image information is not needed at the recovery side. Using user key the recovery process is performed without any loss.

Yongjian and Byeungwoo (2006), propose a visible watermarking system in which the visible watermark helps as a label or rights identifier and it is removed at the recovery side to completely extract the original image. In this study two techniques are proposed. In first one (data hiding), the particular portion of the uncovered image is saved in which the visible watermark image is embedded. To decrease the computational weight, character based arithmetic coding is used. In second one (embedding) a user key is constructed and watermark image is embedded over the reserving portion of the cover image. The watermark removal is done using the user key. The user key is not only used for complete removal of the watermark and also used to serve the hiding information to authorized user.

This visible watermarking technique provides good security and also increases the size of user key.

Soo-Chang and Yi-Chong (2006), implement a watermark removal algorithm to recover an original image using an Independent Component Analysis (ICA) by distinguishing the host image from watermark image and reference image. Three ICA techniques are examined and five visible watermarking methods are carried out to insert consistent and linear-gradient watermarks over the host image. Watermarked image is obtained using a scaling factor and blind removal is performed using reference image which is the mixture of watermarked image and expected visible watermark.

Han-Min and Long-Wen (2007), propose a lossless reversible watermarking by restoring the original image using some special key. Watermark image pixels (bi-level) are embedded with original image using many-to-one mapping technique. The difference image and compressed side information are visibly embedded to restore the original image. Users with correct key can extract original image by removing watermark image.

Han-Min and Long-Wen (2010), proposes a visible watermarking in a secured manner. Pixel mapping embed a watermark over host image. The lost information from watermarking process is treated as recovery data and encrypted with user key to generate an authenticated data. The key generation is based on integer sequence and authentication data and it is embedded with the visible watermarked image. This provides watermark transparency and robust control.

Luo Yong *et al*. (2011), propose a lossless visible watermarking . The key generated at the data hiding side is used to extract watermark image in the receiver side. The Rijndael Hash (RH) arithmetic operator hash function is used by Rijndael encryption algorithm to provide good security.

Non-blind reversible visible watermarking: To recover the original image at the receiver side, original image or watermark signal is required.

Tsung-Yuan and Wen-Hsiang (2010), suggest a reversible one-to-one mapping between visible watermark and host image. Opaque monochrome or color translucent watermark image is embedded into the color image. To recover the image some user key and original watermark signal are considered. Also two-folded reversible mapping is established to avoid deficiency (certain mapping values vary from proposed values) in one-to-one mapping.

In Yongjian *et al*. (2006), propose a removable visible watermark using a user key in DWT domain and allow only authorized user. Lower and higher sub bands are separately considered. To obtain watermarked data, first watermark template is established by pre-processing using user-key, then this template is embedded with host image and host image watermarking coefficients. Watermark removal is reverse of embedding process without host image.

INVISIBLE WATERMARKING

A secrete watermark image is hidden in a host image to carry copyright information or other secret messages. An invisible watermark has very slight change of contrast over large areas of the picture and invisible to the human eyes. For this invisible watermarking , bit rate and signal strength should be low. This study classifies the invisible watermarking into two categories based on robustness as shown in Fig. 2.

Robust invisible watermarking: In this category the watermark removal is very difficult by unauthorized user and it is high resistance to watermarking attacks, hence watermarking attacks never affect the watermarked image.

Ayman and Dwight (2004), Propose a robust invisible watermarking to protect watermarked image from geometric and signal processing attacks. Using an intermediate orthogonal transform, the watermark image is getting embedded into the original image. The Naturalness Preserving Transform (NPT) is used as an intermediate transform in between frequency and spatial domain. Two various NPT forms based on the discrete cosine and Hartley transforms are formulated to improve the image quality. An original image and marked image are required to extract the watermark.

Saraju *et al*. (2007), implement an invisible watermarking technique for Digital Rights Management (DRM). In this study a Discrete Cosine Transform (DCT) domain robust invisible watermarking using cryptography provide two-tier protection against watermarking attacks. Within a color image a binary image is invisibly embedded and private key authentication is also established.

Saraju, *et al*. (2008), propose a new invisible robust watermarking . The watermark is invisibly embedded into a selected region of host image by mixing the composite watermarked image with host image's DCT coefficients. Composite watermark is created by invisibly embedding the watermarked logo (visible) over host image. Watermark extraction is non-blind and correlation detection technique is used to find authentication.

Mnajunatha and Shivaprakash (2010), develop a robust-invisible watermarking using Haar wavelet transform for copyright protection. Watermark embedding and removal is performed using mask matrix. This matrix is established by MD5 algorithm and random matrix generation using the original image.

Xiao-Li *et al*. (2006) implement an invisible watermarking to resist copy attack and common image attacks. Watermark embedding and extraction is performed using Image Independent Block Feature (IIBF) by Independent Component Analysis (ICA) with image signature. It is also used to protect visible watermark image.

Non-robust invisible watermarking: During communication the watermarked image is affected by some set of attacks.

Saba *et al*. (2008), propose an invisible watermarking in both spatial and frequency domain. The watermarking technique in spatial domain is fragile with watermarking attacks and supply pathetic information to unauthorized user. It is used to embed a photographic image and text using Least Significant Bit (LSB) replacement technique. Before insertion preprocessing is performed. The key value is used to locate the points where the watermark information is to be hidden in the host image. Blind water mark extraction is performed using key value.

Soumik *et al*. (2009), propose a novel area to embed color watermark image in host image using various location. The host image is divided into number of blocks

Table 1: Summary- watermarking techniques

Technology		Strength	Weakness
Visible	HVS	Better visual quality	* No limit in recovery packet size
		Good copy right for color images	*Fragile, semi-fragile
	Blind	*Good security	*Rounding error
		*Transparency	*No distortion free
		*Low computational complexity	*Moderate compression.
	Non-blind	*Monochrome, color images.	*Rounding error
		*High visual quality	*No distortion free
Invisible	Robust	*Color to gray scale	*Non-blind
		*Resistant to attacks	
	Non-robust	*Good authentication	*Fragile, semi-fragile

and watermark image is embedded into all blocks of LSB position. Using secrete key and hash function the user will check the user authentication, integrity and ownership. By combining all blocks of LSB values, a fragile technique is developed to extract watermark image.

The consolidated strength and weakness of all the above discussed techniques are tabulated in Table 1.

CONCLUSION

In this study the existing watermarking techniques and their requirements are studied in detail. Based on human perception view, watermarking process is classified into two broad categories. Strength and weakness for all the watermarking techniques are identified and also listed. Generation of novel hybrid techniques is essential to meet out the listed limitations.

ACKNOWLEDGMENT

The authors would like to thank Dr. E. Koperundevi, (Senior Assistant Professor, School of Humanities and Science, SASTRA University) for her valuable suggestions to write this review study.

REFERENCES

Ayman, M.A. and D.D. Dwight, 2004. Applications of the naturalness preserving transform to image watermarking and data hiding. Sci. Direct Digital Signal Process., 14: 531-549.

Biao-Bing, H. and T. Shao-Xian, 2006. A contrast-sensitive visible watermarking scheme. IEEE Multimedia, 13(2): 60-67.

Han-Min, T. and C. Long-Wen, 2007. A High Secure Reversible Visible watermarking Scheme. IEEE International Conference on Multimedia and Expo, pp: 2106-2109.

Han-Min, T. and C. Long-Wen, 2010. Secure reversible visible image watermarking with authentication. Signal Proc. Image Commun., 25(1): 10-17.

Luo Yong., J. Wang, S. Li and X. Liu, 2011. A Lossless and Visible watermarking Algorithm. IEEE Third International Conference on Measuring Technology and Mechatronics Automation, pp: 95-98.

Mnajunatha, P.R. and K. Shivaprakash, 2010. A Robust wavelet-based watermarking scheme for copyright protection of digital images. IEEE Second International Conference on Computing, Communication and Networking Technologies, pp: 1-9.

Min-Jen, T., 2009. A visible watermarking algorithm based on the Content and Contrast Aware (COCOA) technique. J. Vis. Commun. Image R., 20: 323-338.

Soo-Chang, P. and Z. Yi-Chong, 2006. A novel image recovery algorithm for visible watermarked images. IEEE T. Inf. Foren. Sec., 1(4): 543-550.

Soumik, D., P. Bandyopadhyay, S. Paul, A. Sinha Ray and M. Banerjee, 2009. A New Introduction towards Invisible Image watermarking on Color Image. IEEE International Conference on Advance Computing India, pp: 1224-1229.

Saraju, P.M., R. Sheth, A. Pinto and M. Chandy, 2007. Crypt Mark: A Novel Secure Invisible water-marking technique for color images. IEEE International Symposium on Consumer Electronics pp: 1-6.

Saraju, P., B. Mohanty and K. Bhargava, 2008. Invisible watermarking based on creation and robust insertion-extraction of image adaptive watermarks. ACM T. Multimedia Comput. Commun. Appl., 5(2): 22, Article 12.

Saba, R., M. Younus Javed and M. Almas Anjum, 2008. Invisible watermarking Schemes in Spatial and Frequency domains. IEEE International Conference on Emerging Technologies, pp: 211-216.

Tsung-Yuan, L. and T. Wen-Hsiang, 2010. Generic lossless visible watermarking-a new approach. IEEE T. Image Process., 19(5): 1224-1235.

Xiao-Li, N., L. Ju, S. Jian-De and Q. Jian-Ping, 2006. A Novel watermarking Method with Image Signature. Springer-Verlag Berlin Heidelberg, pp: 293-298.

Yongjian, H. and J. Byeungwoo, 2006. Reversible visible water-marking and lossless recovery of original images. IEEE T. Circ. Syst. Video Technol., 16(11): 1423- 1429.

Yongjian, H., K. Sam and H. Jiwu, 2006. An algorithm for removable visible watermarking. IEEE T. Circuits Syst. Video Technol., 16(1): 129-133.

Ying, Y., X. Sun, H. Yang, C.T. Li and R. Xiao, 2009. A Contrast-Sensitive reversible visible image watermarking technique. IEEE T. Circ. Syst., 9: 656-667.