National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)
Proceedings published in International Journal of Computer Applications® (IJCA)

Copyright Protection using Digital Watermarking

Deepa Merin Jose, R.Karuppathal, A.Vincent Antony Kumar
Department of Information Technology
[1,2,3]PSNA College of Engineeringand Technology , Dindigul, TamilNadu, India

ABSTRACT
One way for copyright protection is digital watermarking. Digital watermarking is the process of embedding information regarding the authenticity or the identity of the owners into a image or any piece of data. Digital watermarking has been classified into two types :Visible and Invisible Watermarking. In visible digital watermarking, the embedded information is visible. Typically, the information is text or a logo, which identifies the owner of the image. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it is not visible. Watermarking degrades the quality of an image. By the use of Reversible watermarking the embedded watermark can be removed and restore the original content. The lossless image recovery is a difficult task but; it is important in most of the applications where the quality of the image is concerned. There are many methods for visible watermarking with lossless image recovery. One to One compound mapping is one of the technique. The compound mapping is reversible and it allows lossless recovery of original images from the watermarked images. Security protection measures can be used to prevent illegal attackers.

Keywords
one to one compound mappping, reversible mapping, translucent watermark,opaque watermark, mapping randomization

1. INTRODUCTION
Digital watermarking is the process of embedding information regarding the identity of the owners into an image or any piece of data. It is a special case of information hiding. It is the process of embedding information into digital multimedia content such that the information (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Watermarks are generally used to make it more difficult for people to steal images without giving proper credit. In the recent years due to the growth of Internet it has highlighted the mechanism to protect the ownership of digital media.Digital watermarking has become an active and important area of research and development. Copyright protection for digital information has become easier with the advent of digital watermarking.The information can be textual data about the author,its copyright or image itself. Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. The difference between copy protection and copyright protection. Copy protection limits the access to copyrighted material and inhibit the copy process itself. Examples of copy protection include encrypted digital TV broadcast, access controls to copyrighted software through the use of license servers and technical copy protection mechanisms on the media. A recent example is the copy protection mechanism on DVDs. Copyright protection inserts copyright information into the digital object without the loss of quality. The most prominent way of embedding information in multimedia data is the use of digital watermarking. Digital watermarking can be classified as visible and invisible. The visible watermarks are viewable to the normal eye such as bills, company logos and television channel logos etc. In the case of invisible watermarks, the locations in which the watermark is embedded are secret, only the authorized persons extract the watermark. Some mathematical calculations are required to retrieve the watermark. This kind of watermarks is not viewable by an ordinary eye. Invisible watermarks are more secure and unauthorized user and advertisement. For invisible watermark they can be detected and extracted later to facilitate a claim of ownership ,yielding relevant information as well. Watermarks may also be classified as robust or fragile. Robust watermarks are those which are difficult to remove from the object in which they are embedded, despite various attacks they might be subjected to. By "robust" it means the capability of the watermark to resist manipulations of the media, such as lossy compression , scaling, and cropping**.**

2. LITERATURE REVIEW
Several approaches have been proposed for achieving reversibility.Some of it included a high secure reversible visible watermark algorithm [6]. It can fully remove the watermark from the visible watermarked image such that the original image can be restored. To restore the original image, the difference of subtracting the approximated image from the original image and other side information are losslessly compressed to be embedded in the visible watermarked image by a reversible data embedding algorithm. A key-based scheme is used for the compromise between transparency and robustness. The key is a random variable with discrete normal distribution .Only users with correct key can restore the original image. Digital watermarking[14] is one of the ways to prove the ownership and the authenticity of the media. There are mainly two types of watermarking algorithms: visible watermarking and invisible watermarking. For invisible watermarking, the watermark should be perceptually transparent and robustness. For visible watermarking, the watermark should be perceptually visible and robustness. Watermarking is performed by embedding a digital watermark signal into a digital host signal resulting in watermarked signal. Distortion is introduced into the host image during the embedding process and results in Peak Signal-to-Noise Ratio (PSNR) loss. Reversible watermarking, which can recover the original host signal perfectly after the watermark extraction.There are two lossless visible watermarking algorithms. They are Pixel Value Mapping Algorithm (PVMA) and Pixel Position Shift Algorithm (PPSA). PVMA uses the bijective intensity mapping function to watermark a visible logo whereas PPSA uses circular pixel shift to improve the visibility of the watermark in the high variance region.
Reversible watermarking using perceptual model[11] is used**.** During data hiding, distortions are introduced in an original image because of quantization errors, bit replacement, or truncation at the gray-scale limit. These distortions are irreversible and visible, which is unacceptable in some applications such as medical imaging.A new method for protecting the copyright and verifying the integrity of BMP images[15] by using removable visible watermarks and irremovable visible watermarks.Depending on the relationship between the embedded message and the cover image, data

embedding applications[8] could be divided into two groups. The first group is formed by steganographic applications.The second group of applications is frequently addressed as digital watermarking.In watermarking application, the message supplies additional information about the image, such as image caption, data about the image origin, author signature, image authentication code. There are some applications for which any distortion introduced to the image is not acceptable.A secure algorithm[7] is used for watermarking .Conventional cryptographic systems permit only valid key holders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Therefore conventional cryptography provides little protection against data privacy, in which a publisher is confronted with unauthorized reproduction of information. It is a visible, or preferably invisible, identification code that is permanently embedded in the data.

Circular interpretation of bijective transformations[3] guarantees the coherence of the transformation interpretation and, consequently, ensures total reversibility. Watermarking was designed to meet copyright protection requirements. It is attractive to convey metadata, enabling content indexing, management, and tracing. This technique controls content integrity and authentication, it is referred as fragile. Lossless image processing is used, to extract specific information through extreme zoom. Medical imaging, image archival systems, artworks, military images, and remotely sensed images are all candidates for lossless processing, and watermarking.

The main feature of reversible data embedding [9] is the reversibility. It can remove the embedded data to restore the original image. Here reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original state. The performance of a reversible data-embedding algorithm can be measured by payload capacity limit, visual quality, complexity. Here distortion free data embedding is the main aim of reversible data embedding . If there is any change, it will affect the intelligence of the image, and the access to the original.A new method for copyright protection and authentication of gray scale images[13] by removable visible watermarking and invisible signal embedding techniques is proposed. The involved techniques include a human visual model, least significant bit replacement, and reversible pixel color adjustment. These techniques are integrated effectively to embed a visible watermark and authentication signals into the single grayscale channel of the image. The copyright of the image can be proved by extracting the embedded watermark. And the integrity of the image can be proved by verifying the existence of the embedded authentication signals. By the rapid growth of digital processing techniques, digital images may be duplicated and tampered easily, resulting possibly in unauthorized uses or modifications.

3. DESCRIPTION

A. One to One Compound Mapping

A new method for visible watermarking with a capability of lossless image recovery. The method is based on the use of one to one compound mapping of image pixels value. The compound mapping are reversible and it allows lossless image recovery of original image from the watermarked image. The mappings is adjusted to yield pixels value close to that of desired visible watermarks. Copyright protection for digital information has become easier with use of digital watermarking. Security protection measures can be used to prevent illegal attackers.

B.Lossless Visible Watermarks

Visible watermarking is the easiest way to prove ownership. Embedding distortion in visible watermarking is larger than invisible watermarking, so lossless property is used to ensure signal fidelity. By using lossless watermark the original host image can be recovered after the watermarked extraction process.

The main feature of lossless visible watermark are, the regions with uniform intensity to noise than the regions with the non-uniform intensity. Human visual system is more sensitive to the noise in mid intensity region than that in low intensity region and high intensity region. The watermark should embedded in center position in order to prevent cropping. Visible watermarking is one of the way to prevent illegal use from the unauthorised users by observing the visible logo by human eye. By the use of reversible watermarking, embedded watermark is removed and restore the original content. The recovered image should be identical to the original image, pixel by pixel. Lossless recovery is important in many applications such as forensics, medical image analysis, historical art imaging or military applications.

Several lossless invisible techniques have been proposed. The most common approach is to compress a portion of the original host and then embed the compressed data together with the intended payload into the host . Another approach is to superimpose the spread-spectrum signal of the payload on the host so that the signal is detectable and removable .A third approach is to manipulate a group of pixels as a unit to embed a bit of information. As to lossless visible watermarking, the most common approach is to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT coefficients in the watermark region .Another approach is to rotate consecutive watermark pixels to embed a visible watermark. One advantage of these approaches is that watermarks of arbitrary sizes can be embedded into any host image.

A new method is used for visible watermarking with lossless image i.e, one to one compound mapping. The compound mapping is reversible and recover the original image from watermarked image. The compound mapping allow values to be controllable. The approach is generic, it embed different types of visible watermarks into cover images. Two applications are used, opaque monochrome watermarks and translucent full color are embedded into color images. In visible watermark, only binary visible watermark can be embedded, which is too risk because most of the company logos are colourful.

Fig.1 Original Image and Watermarked image

4. IMPLEMENTATION

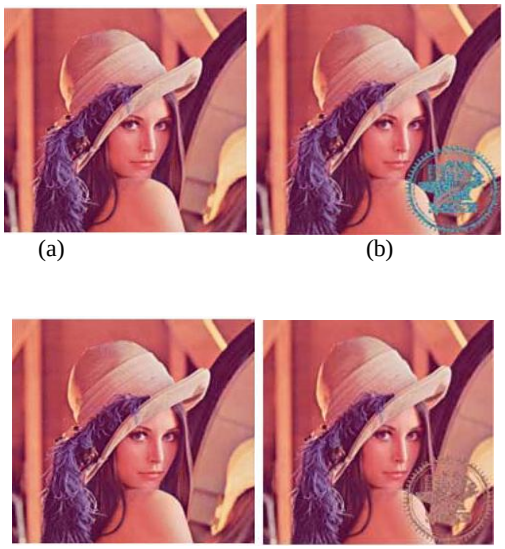
Based on one to one compound mapping ,it can be designed for embedding different types of watermarks into images. The original image can be recovered losslessly from resulting watermark image by using reverse mappings.

A set of values A={a1,a2,a3.....am} into another set B={b1,b2,b3.....bn}, such that mapping from a_i to b_i is reversible. All the values a_i and b_i are image pixel values.The

compound mapping function is one to one function in the following way:

$$F_x(a)=(a-x) \bmod 256, \quad b=F_y^{-1}(F_x(a))$$

This compound mapping is reversible,the watermark can be removed to recover the original image losslessly.The experimental results of embedded watermark and its removal is shown in the figure 2.



(a) (b)

(c) (d)

Fig 2:Experimental results of embedded watermark and removal

Fig 2(a) is the original image.Fig 2(b) is the watermarked image.The image is recovered by using correct keys in shown in Fig 2(c) and those recovered with incorrect keys are shown in Fig 2(d).When the key is incorrect,the inserted watermark cannot remove completely,the noise remain in the watermarking area.

By using lossless watermark the original host image can be recovered after the watermarked extraction process. The main feature of lossless visible watermark are, the regions with uniform intensity to noise than the regions with the non-uniform intensity. Human visual system is more sensitive to the noise in mid intensity region than that in low intensity region and high intensity region. The watermark should embedded in center position in order to prevent cropping. Visible watermarking is one of the way to prevent illegal use from the unauthorised users by observing the visible logo by human eye. By the use of reversible watermarking, embedded watermark is removed and restore the original content. The recovered image should be identical to the original image, pixel by pixel. Lossless recovery is important in many applications such as forensics, medical image analysis, historical art imaging or military applications.

Several lossless invisible techniques have been proposed. The most common approach is to compress a portion of the original host and then embed the compressed data together with the intended payload into the host . Another approach is to superimpose the spread-spectrum signal of the payload on the host so that the signal is detectable and removable .A third approach is to manipulate a group of pixels as a unit to embed a bit of information. As to lossless visible watermarking, the most common approach is to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT coefficients in the watermark region .Another approach is to rotate consecutive watermark pixels to embed a visible watermark. One advantage of these approaches is that watermarks of arbitrary sizes can be embedded into any host image.

A new method is used for visible watermarking with lossless image i.e., one to one compound mapping. The compound mapping is reversible and recover the original image from watermarked image. The compound mapping allow values to be controllable.The approach is generic, it embed different types of visible watermarks into cover images. Two applications are used, opaque monochrome watermarks and translucent full color are embedded into color images. In visible watermark, only binary visible watermark can be embedded, which is too risk because most of the company logos are colourful.

By using compound mapping method, it can be designed for embedding different types of visible watermark into images. By using reverse mappings, the original image can be recovered from watermarked image.

5. CONCLUSION

In this paper,a new method for lossless visible watermarking with a capability of lossless image recovery and the method is one to one compound mapping. The approach is generic by embedding different types of visible watermarks into cover images. Two types of applications are proposed, opaque monochrome watermarks and nonuniformly translucent full color ones. Since translucent full color are non recoverable watermarked image. It aims to recover original image from watermarked image and investigate the feasibility of inserting dual watermarks so that watermarking removing process can be carried out in easy manner without requiring the availability of the original watermark.

6. ACKNOWLEDGMENT

This research is supported in part by AICTE-RPS(8023/BOR/RPS-105/2006-2007) Scheme and a doctoral program from Dept of IT,PSNACET,TN.

7. REFERENCES

[1] B.Mac(2000) 'Lossless multiresolution transform for image authenticating watermarking' presented at the European Signal Processing Conf., Tampere, Finland,.

[2] C. de Vleeschouwer, J. F. Delaigle, and B.Macq(2003),'Circular interpretation of bijective transformations in lossless watermarking for media asset management' IEEE Trans. Multimedia, Vol. 5, No. 1, pp. 97–105.

[3] C. De Vleeschouwer, J. F. Delaigle, and B.Macq(2001),'Circular Interpretation of Histogram for Reversible Watermarking' IEEE Workshop on Multimedia Signal Processing, Cannes, France, pp. 345-350.

[4] D. Zou, Y. Q. Shi, and Z. Ni(2004),Semi-FragileLosslessDigital Watermarking Scheme Based on Integer Wavelet Transform,' IEEE Workshop on Multimedia Signal Processing, Vol. 5, pp. 195-198.

[5] F.A.P.Petitcolas,R.J. Anderson, and M. G. Kuhn(1999), 'Information hiding—A survey' IEEE, Vol. 87, No. 7, pp. 1062– 1078.

[6] H. M. Tsai and L. W. Chang(2007),'A high secure reversible visible watermarking scheme' in IEEE Int. Conf. Multimedia and Expo, Beijing, China, , pp. 2106–2109.

[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon(1997)"Secure spread spectrum watermarking for

multimedia," IEEE Trans. Image Process., Vol. 6, No. 12, pp. 1673–1687.

[8] J. Fridrich, M. Goljan, and R. Du(2002), 'Lossless data embedding—New paradigm in digital watermarking' J. Appl. Signal Process., Vol. 2002,No. 2, pp. 185–196.

[9] J.Tian(2003), Reversible data embedding using a difference expansion,' IEEE Trans. Circuits Syst. Video Technol., Vol. 13, No. 8, pp. 890– 896.

[10] M. Awrangjeb and M. S. Kankanhalli (2003).' Lossless watermarking considering the human visual system,' presented at the Int. Workshop on Digital Watermarking, Seoul, Korea

[11] M.Awrangjeb and M. S.Kankanhali(2005),'Reversible watermarking using a perceptual model,'J. Electron. Imag. Vol. 14, No. 013014.

[12] N. F. Johnson, Z. Duric, and S. Jajodia (2001), ' Information Hiding. Steganography and Watermarking—Attacks and Countermeasures'. Boston, MA: Kluwer.

[13] P. M. Huang and W. H. Tsai(2003), 'Copyright protection, authentication of grayscale images by removable visible watermarking and invisible signal embedding techniques: A new approach,' presented at the Conf. Computer Vision, Graphics and Image Processing, Kinmen, Taiwan, R.O.C.

[14] S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong(2006), 'Lossless visible watermarking,' IEEE Int. Conf. Multimedia and Expo, pp. 853–856.

[15] Y. J. Cheng and W. H. Tsai (2002), 'A new method for copyright and integrity protection for bitmap images by removable visible watermarks and irremovable invisible watermarks' presented at the Int. Computer Symp.— Workshop on Cryptology and Information Security, Hualien, Taiwan, R.O.C.