ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Generic Lossless Visible Watermarking: A Review

Mrunali U. Bhaisare[1], Prof. V.R.Raut[2]

PG Student, Dept. of EXTC, PRMIT&R, Badnera, St. Gadge Baba Amravati University, Maharashtra, India[1]

Dean Academic, Dept. of EXTC, PRMIT&R, Badnera, St. Gadge Baba Amravati University, Maharashtra, India[2]

ABSTRACT: Generic visible watermarking is a method with an ability of lossless image recovery. The method is based on the one to one compound mapping. The method uses deterministic one-to-one compound mappings of image pixel values for superimposing a variety of visible watermarks of random sizes on cover images. Compound mappings are proved to be a reversible technique, and hence allows the lossless recovery of original images from watermarked images. To yield pixel values close to those of preferred visible watermarks the mappings may be adjusted. There are different types of visible watermarks, i.e opaque monochrome visible watermark and translucent full color visible watermark. These are embedded as applications of the proposed common approach. A 2-fold monotonically growing compound mapping is also one of the type of visible watermark which is created and proved to get more distinctive visible watermarks in the watermarked image. In this paper, security protection measures by parameter and mapping randomizations have also been proposed to prevent attackers from criminal image recoveries. Experimental results represents the effectiveness of the future approach are also included.

KEYWORDS:Lossless recovery of reversible visible watermarking, mapping randomization, one-to-one compound mapping, parameter randomization, translucent watermark, two-fold monotonically increasing.

I. INTRODUCTION

Digital watermarking is on high demand for the limited protection which is the efficient way to protect the digital properties recently. This paper review some techniques about digital watermarking(visible as well as invisible) and a new approach of lossless reversible watermarking techniques with strong security is explained. It is a process of embed information in digital signal in a such way that anyone unable easily to remove it. Most of the scheme don't support for removing visible watermark. tentative expected result shows a good result than other methods mathematically.

Watermarking alter the original data I with the watermark data W in such that the original image and the watermark can be improved later. Some of the factors which are related to watermarking are toughness, safety, simplicity, difficulty and capability and some of these are equally exclusive tradeoffs. Robustness is related to the consistency of watermark detection after it has been processed through various signal-processing operations. Security deal with the difficulty of removing the watermark. A scheme is secure if the knowledge of the embedding algorithm does not help for detecting the hidden data bits. Capacity is related to the amount of information which can be embedded in a given cover object. It is important for the watermarked image to be opposing to common image operations to make sure that the hidden information is still retrievable after such alterations. In the second type, defer visible watermarks which are generally clearly visible after common image operations are applied. Also the visible watermarks express ownership information directly on the media and can prevent the attempts of copyright violation.

Generally Visible or invisible Embedding of watermarks, degrade the quality of the host media. Reversible watermarking techniques allow legitimate users to remove the embedded watermark and restore the original content as needed. But not all reversible watermarking techniques guarantee lossless recovery of an image, means the recovered image is identical to the original image, pixel by pixel. Lossless recovery of an image is important in many applications where serious concerns about image quality arise. Some applications are in forensics lab, medical image analysis, historic art imaging, or in military applications.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Digital watermarking's demand is on high for the controlled protection to protect the digital properties efficiently. In this paper there are several techniques about digital watermarking(visible as well as invisible) and also a new approach of lossless reversible watermarking techniques with strong security is explained. It consists of mathematical model. Digital watermarking is a process of embedding information in digital signal in a such a way that No one can easily remove it. Most of the schemes don't support removal of visible watermark. Experimental expected results are better than the mathematical methods. Watermarking alter the original data I with the watermark data W in such a way that the original image and the watermark can be recovered later. Some factors which are related to watermarking are strength, security, simplicity, difficulty and capacity and some of these parameters are mutually exclusive tradeoffs. Strength is related to the consistency of watermark detection after it has been processed through various signal-processing operations. Security deal with the difficulty of removing the watermark. A scheme is a secure scheme if the knowledge of the embedding algorithm does not help in detecting the hidden data bits. Capacity is related to the amount of information that can be embedded in a given cover object. The watermarked image must be resistant to common image operations so that the hidden information is still retrievable after alterations. In the second type, gives the visible watermarks which are generally clearly visible after common image operations are applied. Visible watermarks also convey ownership information directly on the media and can deter attempts of copyright violation. Watermarks Embedding by visible or invisible, corrupt the quality of the host media in general. Reversible watermarking is a technique that allow legitimate users to remove the embedded watermark and restore the original content as per the requirement. All the reversible watermarking techniques do not guarantees of lossless image recovery, that means, the recovered image is identical to the original, pixel by pixel. Lossless recovery is important in many applications where serious concerns about image quality take place. Some examples are forensics, medical image analysis, historical art imaging, or military applications as compared to the invisible counterpart

II. RELATED WORK

There are two types of methods of Digital watermarking for images which are usually categorized into two types that are invisible and visible. The invisible watermarking method's aim is to embed copyright information slightly into the host media such that in the case of copyright infringements, the hidden information can be retrieve to identify the ownership of the protected host. The watermarked image should be resistant to the common image operations to ensure that the hidden information is still retrievable after such alterations. The second method i.e. visible watermarking, yields the visible watermarks which are generally clearly visible after common image operations are applied and also, visible watermarks convey ownership information directly on the media and can deter attempts of copyright violations.

The reproduction and distribution of digital information became easier than ever before by the advancement of computer technologies and the proliferation of the Internet. Hence the Copyright protection of logical properties has become an important topic. Copyright protection is one of the way of digital watermarking ([1],[2]), which means that the embedding of certain specific information about the copyright holder (company logo, ownership images, etc.) into the media is to be protected. Digital methods of watermarking for images are of two types i.e. invisible and visible. The first type i.e. the invisible watermarking aims is to insert the copyright information invisibly into host media such that in cases of copyright infringements, the hidden information can be retrieved to identify the ownership of the protected host. It is important for the watermarked image to be resistant to common image operations to ensure that the hidden information is still to be retrievable after such alterations. The Visible watermarking is of the second type, gives the visible watermarks which are generally clearly visible after common image operations are applied. Visible watermarking also convey the ownership information directly on the media and can prevent attempts of copyright violation.

Watermarks Embedding either by visible or invisible, degrade the quality of the host media in general. Reversible watermarking technique ([3]–[4]), allow legitimate users to remove the embedded watermark and restore the original content as needed. But not all reversible watermarking techniques guarantee lossless image recovery, that means recovered image is identical to the original, pixel by pixel. Lossless recovery of an image is important in many applications where serious concerns about image quality ARISE. SOME OF THE EXAMPLES INCLUDE IN THE FORENSIC LABS, IN MEDICAL IMAGE ANALYSIS, HISTORIC ART IMAGING, OR IN MILITARY APPLICATIONS.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Compared with the invisible watermarking, there are relatively few mentions of lossless visible watermarking in the literature. Several techniques have been proposed in the past for lossless invisible watermarking. The common approach to compress a portion of the original host and then embedding the compressed data together with the intended payload into the host ([5],[6],[7]). Another approach is to superimpose the spread-spectrum signal of theconsignment on the host so that the signal is detectable and also the removable [8]. The third approach is to manipulate a group of pixels as a unit to embed a bit of the information ([9], [10]). One can use lossless invisible techniques to embed removable visible watermarks [11], [12], but the low embedding capacities of these techniques obstruct the possibility of implanting large sized visible watermarks into host media. Whereas, in the lossless visible watermarking, the common approach to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT coefficients in the watermark region [13], [14], [15]. In the another approach is to rotate the consecutive watermark pixels to embed a visible watermark [15]. One of the advantage of these approaches is that watermarks of illogical sizes can be embedded into any host image. However, using these approaches only binary visible watermarks can be embedded, which is too restrictive hence most of company's logos are colorful.

III. PROPOSED ALGORITHM

Problem Definition:

A digital watermark security refers to the inability of the unauthorized users to modify, remove, detect or estimate the watermark. The aim of an attacker is usually to eliminate, remove or degrade the effectiveness of the watermark, to disable the detector or to attack the concept of the watermarking application. An attack is considered successful if the attacker disrupt any stage of the watermarked life cycle (see Fig. 1). Hence, the content owner and the watermarking software have to ensure that each stage is secured against such manipulations., their security properties have to fulfill different requirements Depending on the watermarks applications. In ensuring the ability of watermarking techniques to get these requirements, it is essential to recognize all possible risks and make some assumptions about the capabilities of the adversary also. For ex. if the opposition knows nothing about the watermarking algorithm, he or she must rely on general knowledge of the weakness from which most watermarking algorithms bear. In some cases, adversary can obtain more than one watermarked image. The enemy can often utilize this situation to remove watermarks, even when he/ she does not know the algorithm (e.g. collusion attacks). For the systems that require a very high level of security, it's better to assume that the opponent knows everything about the algorithm separately from one or more secret keys. Such opponent can find and exploit weaknesses in the detection strategy. In some cases, we can assume that the adversary has a watermark detector. If the enemy knows zero about the algorithm, right of entry to a detector gives him/ her an advantage in attacking the watermark.

An attack is described as any processing that circumvent the intended purpose of the watermarking technique for a given application. Watermarking attacks include normal processing operations, like image compression, and accidental damage of the watermark. These distortions are insufficient to those that do not produce excessive poverty, otherwise the changed object would be unusable. Researchers recognize many types of possible attacks on watermarking schemes, each of them uses a different stage of the watermarking process.

The proposed approach to lossless reversible visible watermarking is based on appropriate one-to-one compound mappings which can be designed to embed different types of visible watermarks into images. By using the corresponding reverse mappings, the original image can be recovered losslessly from a resulting watermarked image.
In lossless visible watermarking, monochrome watermark is embedded or removed in the watermark region is purely based on correct or incorrect keys. Also various types of watermarks are embedded using one to one compound mapping technique which has given in the form of basic algorithm shown below and watermarks of arbitrary sizes also can be embedded into any host image. Only binary visible watermarks can be embedded using these approaches, which is moreover limiting, hence most company logos are colorful. The secret key generated here is by using the Hash Algorithm. The typical watermarking system model is given below. In this paper secret key is generated for watermarking using the HASH algorithm

Hash algorithms are used to provide information security services. Hash functions are regularly use with algorithms of digital signature, message of keyed-hash authentication codes, key derivation functions, and random number generations. A hash algorithm convert the changeable length message into the strong representation of the electronic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

data in the message. A Message digest which is used for digital signatures, authentication of message, and other secure applications. When used in a digital signature application, the hash value of the message is sign as an substitute of the message itself. To verify the signer of the message and also to validate the integrity of the message, the receiver can use the signature.

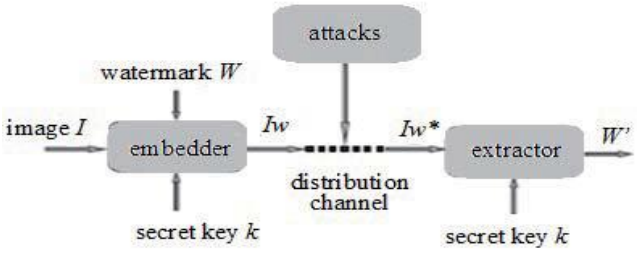

Fig.(1) : Typical watermarked system model

Reversible One-to-One Compound Mapping

First, we propose a generic one-to-one compound mapping for converting a set of numerical values P={p1,p2,p3,.....pM} to another set Q={q1,q2,q3,.....qM}, such that the respective mapping from pi to qi for all {i=1,2,3....M} is reversible. Here, for the copyright protection applications, all values of pi and qi are the image pixel values (grayscale or color values). The compound mapping f is a one-to-one function Fx with one parameter x=a or in the following way:

$q = f(p) = q = F_b^{-1}(F_a(p))$ eqn(1)

where F_b^{-1} is inverse of Fb leads form one to one property leads to the fact that if (Fa(p)) = (p)inverse , then for (Fa(p)) inverse = p for all values of a and p. On the other hand, Fa(p) and Fb(p) generally are set to be unequal if 'a' is not equal to 'b' .

The compound mapping described by eqn. (1) is reversible, which is p, and can be derived exactly from q using the following formula:

$p = f(q) = p = F_a^{-1}(F_b(q))$ eqn.(2)

Lemma 1 (Reversibility of Compound Mapping):

If $q = F_b^{-1}(F_a(p))$ for any one-to-one function F_x with a parameter x, then $p = F_a^{-1}(F_b(q))$ for any values of a, b, p and q.

Proof: Substituting (1) into $F_a^{-1}(F_b(q))$, we get

$$F_a^{-1}(F_b(q)) = F_a^{-1}\left(F_b\left(F_b^{-1}(F_a(p))\right)\right).$$

By regarding $F_a(p)$ as a value c, the right-hand side becomes, $F_a^{-1}\left(F_b(F_b^{-1}(c))\right)$, which, after F_b and F_b^{-1} are cancelled out, becomes $F_a^{-1}(c)$. But $F_a^{-1}(c)=F_a^{-1}(F_a(p))$, which is just p after F_a and F_a^{-1} are cancelled out. That is, we have proved $p = F_a^{-1}(F_b(q))$.

As an example,

If $F_x(p) = xp + d$, then $F_x^{-1}(p') = (p' - d)/x$.

Thus

$q = F_b^{-1}(F_a(p)) = F_b^{-1}(ap + d) = [(ap + d - d)/b] = ap/b$

and so, we have

$F_a^{-1}(F_b(q)) = F_a^{-1}\left(b\left(\frac{ap}{b}\right) + d\right) = F_b^{-1}(ap + d) = [((ap + d) - d)/a] = (ap/a)$ =pas expected by Lemma1.

Algorithms

1. **Embedding of Generic Visible Watermark**
2. **Generic Watermark Removal for Lossless Image Recovery**
3. **Watermark Embedding of a Translucent Color Watermark**
4. **One-to-One Mapping Exhibiting One-Fold Monotonically Increasing Property**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

IV. PSEUDO CODE

Algorithm 1: Embedding of Generic Visible Watermark
Input: an image **I** and a watermark **L**.
OUTPUT: watermarked image
Steps:

1) Select a set of pixels P from I where L is to be embedded, and call a P watermarking area.

2) Denote the set of pixels corresponding P to in W by Q .

3) For each pixel of X with the value p in the P region , denote the corresponding pixel in Q as Z and the value of the corresponding pixel in as , and conduct the following steps.

a) By applying an estimation technique to derive a to be a value close to p , using the values of the neighbouring pixels of X (excluding X itself).

b) Set b to be the value L .

c) Map to a new value $q = F_b^{-1}(F_a(p))$

d) Set the value of Z to be q .

4) Set the value of each remaining pixel in W , whichis outside the region P , to be equal to that of the corresponding pixel in I

Algorithm 2: Generic Watermark Removal to Recoverthe Lossless Image
Input: A watermarked image W and a watermark L.
Output: the original image R is recovered from W.
Steps:

1) Select the same watermarking area Q in W as that of Algorithm 1.

2) Set the value of each pixel in R , to be equal to that of the corresponding pixel In W,which is outside the Region Q.

3) For each pixel Z with value Q in q , denote the corresponding pixel in the recovered image R as X and the value of the corresponding pixel Y in L as l, and conduct the following steps.

a) By applying the same estimation technique used obtain the same value as that derived in Step 3a of Algorithm 1

b) Set b to be the value L.

c) Restore from by setting, $p = F_a^{-1}(F_b(q))$

d) Set the value of X to be p .

V. SIMULATION RESULTS

The following two images shows how the mapping is done on the colorimage the embedding of watermark for different types of watermarks.

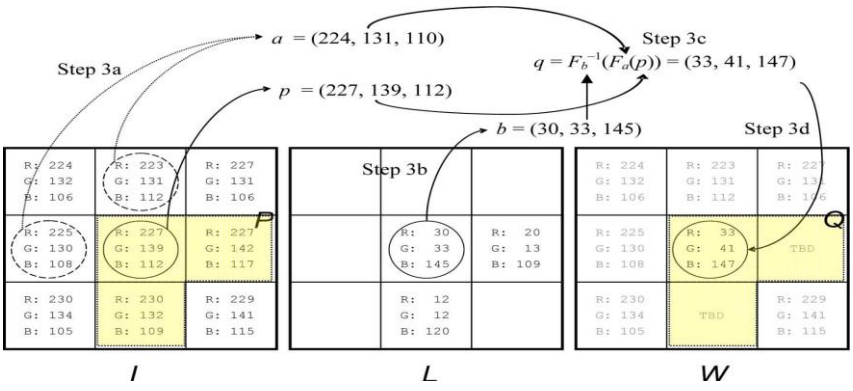

Fig. (2). Illustration of mapping the center pixel of a 3x3 image using Algorithm 1. Only the mapping of the center pixel is shown for clarity; the east and sout pixels are depicted as TBD (to be determined) in W.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

In fig. 2, the I is the original image, L is the Watermark and W is the watermarked image after embedding. In this fig, first we assigned the watermarking area in I where we have to place the watermark, the remaining pixels will remain the same. The a parameter is selected such that it is the north west pixels of P, and a is obtained by averaging the north west pixels of watermarking area P. b will be the pixels of watermark. Then by one to one compound mapping is used to get the values of p and q, the procedure is explained in the above algorithm1. Hence we get the following image as a result of algorithm 1

(a) (b) (c)

Fig.(3). Illustration of pixels in a watermark. (a) A monochrome watermark. (b) Area of p (yellow pixels). (c) Area of p' (yellow pixels).

Fig 3 shows the different types of watermarks. In the fig. 3 (a) is the opaque type of watermark is there. In 3(b) is the watermarked image where watermark is of the type monochrome color watermark and in fig 3.(c) is the transculent type of watermark is used for watermark embedding.

VI. CONCLUSION AND FUTURE WORK

A new method has been proposed for the reversible visible watermarking for lossless image recovery capability. This method uses one to-one compound mappings which can plot the image pixel values to those of the desired visible watermarks. To demonstrate the reversibility of the compound mappings for lossless reversible visible watermarking. Here used are two algorithms for watermarking and removing watermark to get the original image back. Hence by using these two algorithms of watermark embedding and removal of watermark to get the original image back we get the recovered image exactly similar to that of the original image pixel by pixel. The future work will be based on the next two algorithms i.e.Watermark Embedding of a Translucent Color Watermark, One-to-One Mapping Exhibiting One-Fold Monotonically Increasing Property for digital watermarking

REFERENCES

1. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "*Information hiding—A survey*," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.
2. G. Braudaway, K. A. Magerlein, and F. Mintzer, "*Protecting publicly available images with a visible image watermark*," in Proc. SPIE Int. Conf. Electronic Imaging, Feb. 1996, pp. 126–133, vol. 2659.
3. Y. J. Cheng and W. H. Tsai, "*A new method for copyright and integrity protection for bitmap images by removable visible watermark and irremovable invisible watermarks*," presented at the Int. Compute Symp.—Workshop on Cryptology and Information Security, Hualien Taiwan, R.O.C., Dec. 2002
4. S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, "*Lossless visible watermarking*," in Proc. IEEE Int. Conf. Multimedia and Expo, pp. 853–856, Jul. 2006.
5. Y. Hu and S.Kwong,"*Wavelet domain adaptive visiblewatermarking*," Electron. Lett., vol. 37, no. 20, pp. 1219–1220, Sep. 2001.
6. J. Fridrich, M. Goljan, and R. Du, "*Lossless data embedding—New paradigm in digital watermarking*," J. Appl. Signal Process., vol. 2002, no. 2, pp. 185–196, Feb. 2002.
7. M. Awrangjeb and M. S. Kankanhalli, "*Reversible watermarking using a perceptual model*," J. Electron. Imag., vol. 14, no. 013014, Mar. 2005.
8. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "*Secure spread spectrum watermarking for multimedia*," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Jun. 1997.
9. C. de Vleeschouwer, J. F. Delaigle, and B. Macq, "*Circular interpretation of bijective transformations in lossless watermarking for media asset management*," IEEE Trans. Multimedia, vol. 5, no. 1, pp. 97–105,Mar. 2003.
10. J. Tian, "*Reversible data embedding using a difference expansion*," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
11. Y. Hu and B. Jeon, "*Reversible visible watermarking and lossless recovery of original images*," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 11, pp. 1423–1429, Nov. 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

12. H. M. Tsai and L. W. Chang, "*A high secure reversible visible watermarking scheme*," in Proc. IEEE Int. Conf. Multimedia and Expo, Beijing, China, pp. 2106–2109, Jul. 2007.
13. S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "*A DCT domain visible watermarking technique for images*," in Proc. IEEE Int. Conf. Multimedia and Expo, vol. 2, pp. 1029–1032,Jul. 2000.
14. P. M. Huang and W. H. Tsai, "*Copyright protection and 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., Aug. 2003.
15. S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, "*Lossless visible watermarking*," in Proc. IEEE Int. Conf. Multimedia and Expo, pp. 853–856,Jul. 2006.
16. Tsung-Yuan Liu, "*Generic Lossless Visible Watermarking*", Student Member, IEEE, and Wen-Hsiang Tsai, Senior Member, IEEETRANSACTIONS ON IMAGE PROCESSING, VOL. 19, NO. 5, MAY 2010

BIOGRAPHY

Mrunali Udaram Bhaisare is a Post Graduate Student of Elecronics and Telecommunication Department for the Master of Engineering Course in college of Prof. Ram Meghe Institute of Technology and Research Badnera, Saint Gadge Baba Amravati University. She received Bachelor of Engineering degree in 20 from RMCET, Mumbai University, Ratnagiri MS, India. Her research interests is Image Processing.