Generic Lossless Visible Watermarking

Kushmeen P. Gurudatte[1], Manju D. Pawar[2]

[1, 2]Department of ECT, Marathwada Institute of Technology, Aurangabad, India

Abstract: ***A novel method for generic visible watermarking with a capability of lossless image recovery is proposed. The method is based on the use of deterministic one-to-one compound mappings of image pixel values for overlaying a variety of visible watermarks of arbitrary sizes on cover images. The compound mappings are proved to be reversible, which allows for lossless recovery of original images from watermarked images. The mappings may be adjusted to yield pixel values close to those of desired visible watermarks. Different types of visible watermarks, including opaque monochrome and translucent full color ones, are embedded as applications of the proposed generic approach. A two-fold monotonically increasing compound mapping is created and proved to yield more distinctive visible watermarks in the watermarked image. Security protection measures by parameter and mapping randomizations have also been proposed to deter attackers from illicit image recoveries. Experimental results demonstrating the effectiveness of the proposed approach are also included.***

Keywords: Lossless reversible visible watermarking, mapping randomization, one-to-one compound mapping, parameter randomization, translucent watermark, two-fold monotonically increasing

1. Introduction

The advance of computer technologies and the proliferation of the Internet have made reproduction and distribution of digital information easier than ever before. Copyright protection of intellectual properties has, therefore, become an important topic. One way for copyright protection is digital watermarking, which mean embedding of certain specific information about the copyright holder (company logos, ownership descriptions, etc.) into the media to be protected. Digital watermarking methods for images are usually categorized into two types: invisible and visible. The first type aims to embed copyright information imperceptibly 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 retrievable after such alterations. Methods of the second type, on the other hand, yield visible watermarks which are generally clearly visible after common image operations are applied. In addition, visible watermarks convey ownership information directly on the media and can deter attempts of copyright violations.

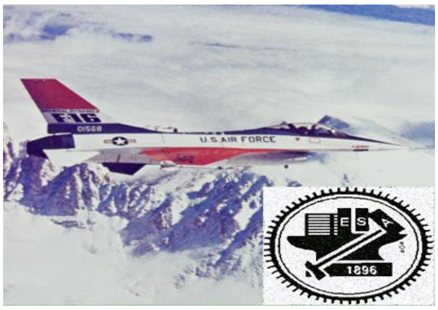


Figure 1: A watermarked image

Embedding of watermarks, either visible or invisible, degrade the quality of the host media in general. A group of techniques, named reversible watermarking, allow legitimate users to remove the embedded watermark and restore the original content as needed. However, not all reversible watermarking techniques guarantee lossless image recovery, which means that the recovered image is identical to the original, pixel by pixel. Lossless recovery is important in many applications where serious concerns about image quality arise. Some examples include forensics, medical image analysis, historical art imaging, or military applications. Compared with their invisible counterparts, there are relatively few mentions of lossless visible watermarking in the literature. Several lossless invisible watermarking techniques have been proposed in the past. 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. Although one may use lossless invisible techniques to embed removable visible watermarks, the low embedding capacities of these techniques hinder the possibility of implanting large-sized visible watermarks into host media. 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.

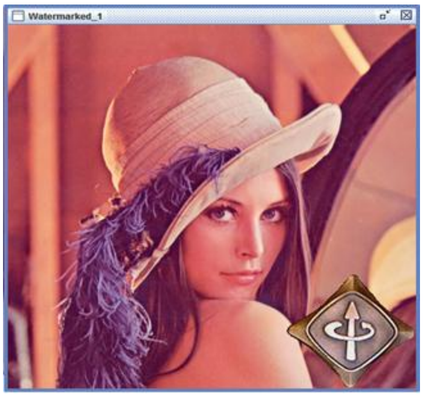


Figure 2: Watermarked image as benchmark image

Licensed Under Creative Commons Attribution CC BY

However, only binary visible watermarks can be embedded using these approaches, which is too restrictive since most company logos are colorful. In this paper, a new method for lossless visible watermarking is proposed by using appropriate compound mappings that allow mapped values to be controllable. The mappings are proved to be reversible for lossless recovery of the original image. The approach is generic, leading to the possibility of embedding different types of visible watermarks into cover images. Two applications of the proposed method are demonstrated, where opaque monochrome watermarks and no uniformly translucent full-color ones are respectively embedded into color images. More specific compound mappings are also created and proved to be able to yield visually more distinctive visible watermarks in the watermarked image. To the best knowledge of the authors, this is the first method ever proposed for embedding removable translucent full-color watermarks which provide better advertising effects than traditional monochrome ones.

Algorithm

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.
5) Inverse of the mapping function of One-to-One Mapping Exhibiting One-Fold Monotonically Increasing Property.

Algorithm 1

Generic Visible Watermark Embedding
Input- an image I and a watermark L.
Output- Watermarked image W

Steps:

1) Select a set P of pixels from I where L is to beembedded and call P a watermarking area.
2) Denote the set of pixels corresponding to p in W by Q.
3) For each pixel X with value p in P, denote the corresponding pixel in Q as Z and the value of the corresponding pixel y in L as l and conduct the following steps.
   a) Apply an estimation technique to derive a tobe 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 p to be a value q=Fb-1(Fa (p))
   d) Set the value of Z to be q.
4) Set the value of each remaining pixel in Wwhich is outside the region P to be equal to that of the corresponding pixelon I.

Algorithm 2

Generic Watermark Removal for lossless image recovery.
Input- Watermarked image W and a watermark L.
Output- original image R recovered by W

Steps:

1) Select the same watermarking area.Q in w as that selected in algorithm 1
2) set the value of each pixel in R , which is outside the region Q to be equal to that of the corresponding pixels in W
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) Obtain the same value a as that derived in step 3 of algorithm 1 by applying the estimation technique used there.
   b) Set b to be the value l.
   c) Restore p from q by setting p=Fa-1(Fb(q))
   d) Set the value of X to be p.

Algorithm 3

Watermark embedding of a translucent color watermark.
Input- image I and a translucent Watermark L
Output- watermarked image W
Steps:

1) Select the watermarking area.P in l to be the set of pixels corresponding spatially to those in L which are non transparent (with alpha value larger than zero)
2) Denote the set of pixels corresponding to P inW as Q.
3) For each pixel X with value p in P, denote the corresponding pixel in Q as Z and the value of the corresponding pixel Y in L as l and conduct the following steps.
   a) Set the parameter a to be a neighbour based ccolor estimate value that is close to p by using the colors of the neighbouring pixels of X that have already been processed.
   b) Perform alpha blending with l over a to get the parameter b according to the formula b=l*a+a*(255-a) where a is the opacity of Y
   c) Map p to a new value q =Fb-1(Fa(q))
   d) Set the value of Z to be a.

Algorithm 4

One to one mapping exhibiting of a monotonically increasing property
Input- A parameter a and an input value p, each in the range of 0 to 255.
Output- a mapped output p’ in the range from 0 to 255

Steps:

1) Initialize p’ to be zero.
2) Create a set S with initial elements being the 256 values of 0 through 255.
3) Find a value r in S such that a-r is the minimum preferring a smaller r in case of ties.
4) If r is not equal to p, then remove r from S , increment p’ by one, and go to step 3; otherwise, take the final p’ as output.

Algorithm 5 Inverse of the mapping function described by algorithm.
Input- A parameter b and an input value p’, each in the range of 0 to 255.
Output- an output value p in the range from 0 to 255

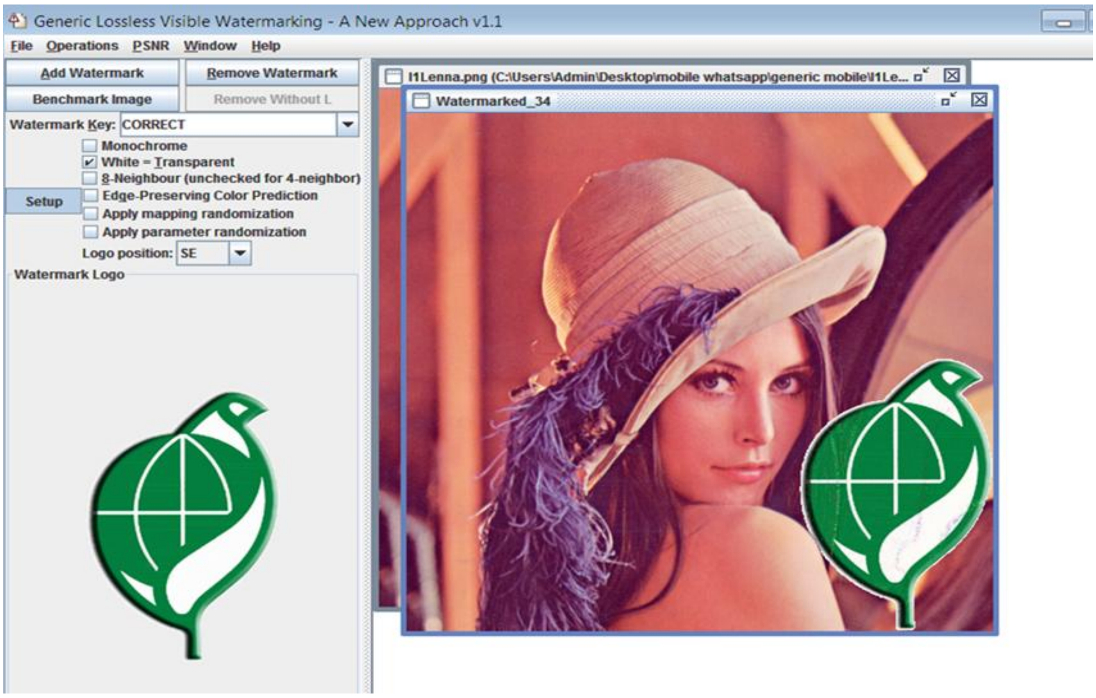
Steps:

a) Create a set S with initial elements being the 256 values of 0 through 255.

Licensed Under Creative Commons Attribution CC BY

b) find a value p in S such that b-p is the minimum preferring a smaller p in case of ties.

c) If p' is larger than zero, then remove p from S, decrement p' by one, and go to step 2; otherwise, take the final p as output.


Generic Lossless Visible Watermarking - A New Approach v1.1
File
Operations
PSNR
Window
Help
Add Watermark
Remove Watermark
Benchmark Image
Remove Without L
Setup
Watermark Logo
I1Lenna.png (C:\Users\Admin\Desktop\mobile whatsapp\generic mobile\I1Le...
Watermarked_34

Watermark Key: CORRECT

☐ Monochrome
☑ White = Transparent
☐ 8-Neighbour (unchecked for 4-neighbor)
☐ Edge-Preserving Color Prediction
☐ Apply mapping randomization
☐ Apply parameter randomization

Logo position: SE

Figure: watermarking done for any general arbitrary sized watermark

2. Security Consideration

Though we want legitimate users to be able to recover the original image from a watermarked one, we do not want an attacker to be able to do the same. Herein, we propose some security protection measures against illicit recoveries of original images. First, we make the parameters a and b in the above algorithms to be dependent on certain secret keys that are known only by the creator of the watermarked image and the intended receivers. One simple technique to achieve this is to use a secret key to generate a pseudo-random sequence of numerical values and add them to either or both of a and b for the pixels in the watermarking area. This technique is hereinafter referred to as parameter randomization.

Another way of security protection is to make the choices of the positions for the pixels to be dependent on a secret key. Specifically, we propose to process two randomly chosen pixels (based on the security key) in P simultaneously as follows. Let the two pixels be denoted as X1 and X2 with values p1and p2, respectively.

$$q_1 = F_{b_1}^{-1}(F_{a_2}(p_2)) \quad \text{and} \quad q_2 = F_{b_2}^{-1}(F_{a_1}(p_1)).$$

The parameter exchange does not affect the effectiveness of lossless recoverability because we can now recover the original pixel values.

$$p_1 = F_{a_1}^{-1}(F_{b_2}(q_2)) \quad \text{and} \quad p_2 = F_{a_2}^{-1}(F_{b_1}(q_1)).$$

We will refer to this technique in the sequel as mapping randomization. We may also combine this technique with the above- mentioned parameter randomization technique to enhance the security further.

Last, the position in the image where a watermark is embedded affects the resilience of the watermarked image against illicit image recovery attempts. In more detail, if the watermark is embedded in a smooth region of the image, an attacker can simply fill the region with the background color to remove the watermark irrespective of the watermarking technique used. To counter this problem, an appropriate position should be chosen, using, for example, the adaptive positioning technique when embedding a watermark. However, for ease of discussions and comparisons, we always embed a watermark in the lower hand corner of an image.

3. Experimental Results

A series of experiments implementing the proposed methods were conducted using the Java SE platform. To quantitatively measure the effectiveness of the proposed method, we define a set of performance metrics here. First, the quality of a watermarked image W is measured by the peak signal-to-noise ratio(PSNR) of W with respect to the non recoverable watermarked image B in the following way:

$$\mathrm{PSNR}_W = 20 \times \log_{10}\left(255 \bigg/ \sqrt{\frac{1}{w \times h}\sum_{y=1}^{h}\sum_{x=1}^{w}[W(x,y) - B(x,y)]^2}\right)$$

Also, the quality of a recovered image R is measured by the PSNR of R with respect to the original image I in a similar way

$$\mathrm{PSNR}_R = 20 \times \log_{10}\left(255 \bigg/ \sqrt{\frac{1}{w \times h}\sum_{y=1}^{h}\sum_{x=1}^{w}[R(x,y) - I(x,y)]^2}\right)$$

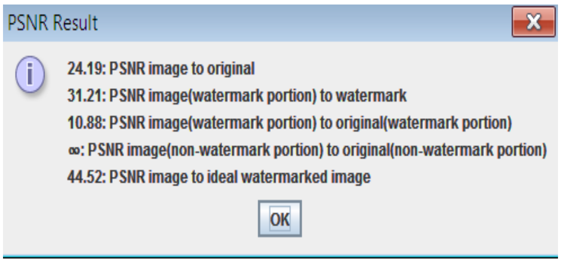
It is desired to have the value of the PSNRw to be as high as possible, so that the watermarked image can be visually as close to the benchmark image as possible. For illicit

Licensed Under Creative Commons Attribution CC BY

recoveries, the PSNRr should be as low as possible to make the recovered image visually intolerable (e.g., very noisy). In particular, we want the region obscured by the watermark to be as noisy as possible in an illicitly recovered image. For this purpose, we introduce an additional quality metric for an illicitly recovered image that only takes into account the region Q covered by the watermark. Specifically, we measure the quality of the recovered image by the following PSNR measure:.

$$\mathrm{PSNR}_Q = 20 \times \log_{10}\left(255 \Big/ \sqrt{\frac{1}{|Q|}\sum_{y=1}^{h}\sum_{x=1}^{w} SE_Q(x,y)}\right)$$

Six test images, each of dimensions 512* 512, were used in the experiments. The color estimate of a pixel was derived by averaging the available four-neighbors of that pixel. Such an experiment was conducted twice to test the effectiveness of the two proposed security protection measures: the mapping and the parameter randomization techniques. For the latter, both the parameters and of the compound mapping were adjusted randomly within a range of 25 with a uniform probability distribution. A total of watermarked images were generated and for each watermarked image, recoveries using correct as well as incorrect keys were conducted.



PSNR Result

24.19: PSNR image to original
31.21: PSNR image(watermark portion) to watermark
10.88: PSNR image(watermark portion) to original(watermark portion)
∞: PSNR image(non-watermark portion) to original(non-watermark portion)
44.52: PSNR image to ideal watermarked image

Figure PSNR values of the image and the watermarks

Here we are finding the PSNR values of the image and the watermark. Here we compare the PSNR values of an benchmark image to the PSNR values of the watermarked image obtained by using any of the algorithms used above. Here we will find the PSNR value of the image to original, watermark portion to watermark, image watermark portion to original watermark portion, image non watermark portion to original non-watermark portion, image to ideal watermarked image.In the above fig. the PSNR values are compared and demonstrated .Here we can find the values for all types of the watermarks be it a watermark of any arbitrary size or a coloured translucent watermark , an opaque watermark or any coloured watermark or a monochrome one here the values helps us to the decide the lossless character of the image .PSNR which is the peak signal to noise ratio help us to compare all the values and also has the MSE values to calculate the PSNR and the formula to find out these values is mentioned above.

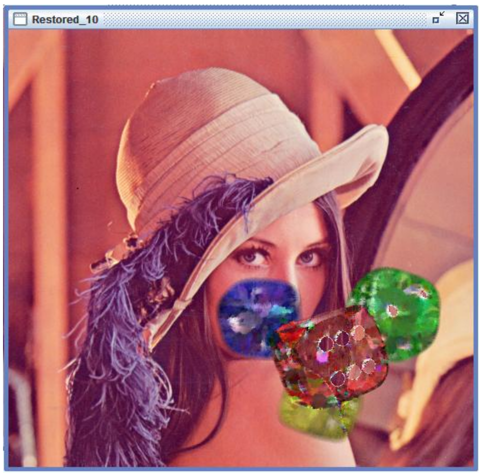
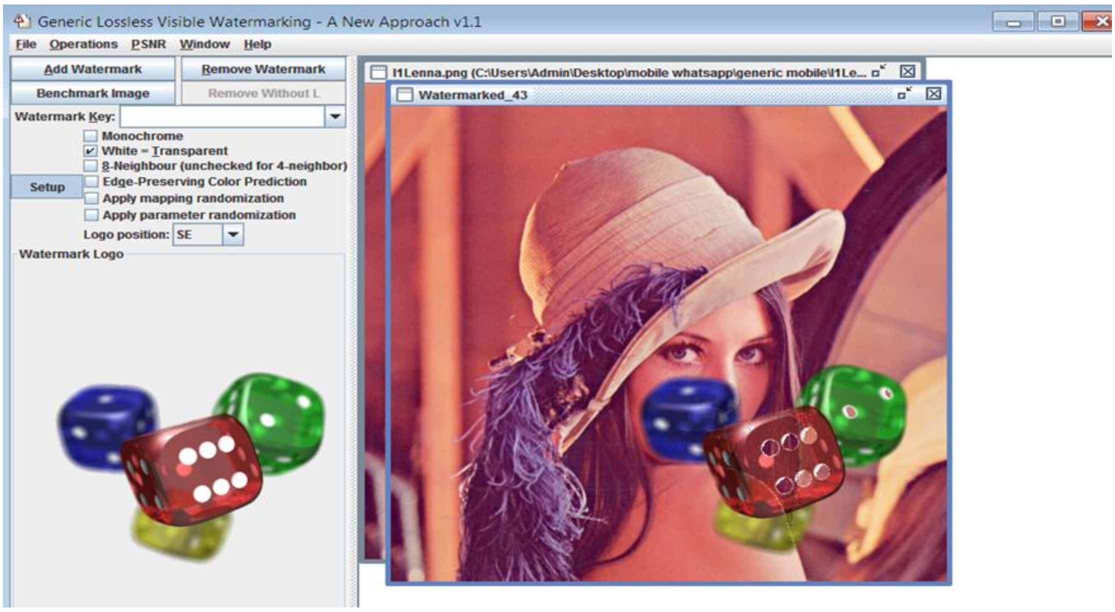


Fig trying to recover the image with wrong key

4. Security Increase Results

For the purpose of the increase in the security of the watermarking done to transfer the right information of eg. A company logo a lot of security measures have been applied as shown above and as an additional security measure to prevent the illicit recovery of the watermark by any unknown user we have added password security and if the password entered by the user is wrong then the image recovery is not possible as shown in fig the image gets damaged or blurred and loses the important information it wishes to convey and in appearance the image looks damaged. Here in this paper we have shown the examples of trying of illicit recovery and their results for any arbitrary image or coloured translucent watermark or an opaque watermark.

Licensed Under Creative Commons Attribution CC BY



Generic Lossless Visible Watermarking - A New Approach v1.1
File
Operations
PSNR
Window
Help
Add Watermark
Remove Watermark
Benchmark Image
Remove Without L
Setup
Watermark Logo
I1Lenna.png (C:\Users\Admin\Desktop\mobile whatsapp\generic mobile\I1Le...
Watermarked_43

Watermark Key:

□ Monochrome
☑ White = Transparent
□ 8-Neighbour (unchecked for 4-neighbor)
□ Edge-Preserving Color Prediction
□ Apply mapping randomization
□ Apply parameter randomization

Logo position: SE

Figure: Watermarked image for coloured translucent watermark

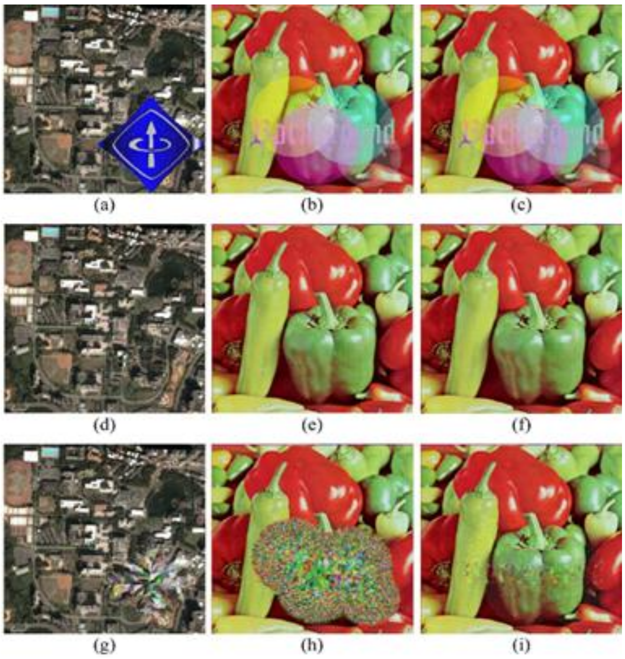


Figure: Watermarked image, licitly recovered image and illicitly recovered image, a-c watermarked image ,d-f licitly recovered image from images a-c , illicitly recovered image from images a-c respectively

5. Conclusion and Future Scope

In this project, a new method for reversible visible watermarking with lossless image recovery capability has been proposed. The method uses one-to-one compound mappings that can map image pixel values to those of the desired visible watermarks. Relevant lemmas and theorems are described and proved to demonstrate the reversibility of the compound mappings for lossless reversible visible watermarking. The compound mappings allow different types of visible watermarks to be embedded, and two applications have been described for embedding opaque monochrome watermarks as well as translucent full-color ones. Translucent watermarks clearly visible and visually appealing, thus more appropriate than traditional transparent binary watermarks in terms of advertising effect and copyright declaration. The two-fold monotonically increasing property of compound mappings was defined and an implementation proposed that can provably allow mapped values to always be close to the desired watermark if color estimates are accurate. Also described are parameter randomization and mapping randomization techniques, which can prevent illicit recoveries of original images without correct input keys. Experimental results have demonstrated the feasibility of the proposed method and the effectiveness of the proposed security protection measures.

References

[1] Tsung-Yuan Liu, Student Member, IEEE, and Wen-Hsiang Tsai Senior Member, IEEE . Generic Lossless Visible Watermarking—A New Approach. IEEE Transactions on image processing, Vol. 19, no. 5, may 2010

[2] International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 1, January 2015 Copyright to IJIRCCE 10.15680/ijircce.2015.0301018 340Generic Lossless Visible Watermarking: A review

[3] International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 1, January2015Generic Lossless Visible Watermarking: A ReviewMrunali U. Bhaisare1, Prof. V.R.Raut

[4] A. Lumini and D. Maio, “Adaptive positioning of a visible watermarking a digital image,” in Proc. Int. Conf. Multimedia and Expo, Taipei,Taiwan, R.O.C., Jun. 2004, pp. 967–970.

[5] Y. Hu, S. Kwong, and J. Huang, “An algorithm for removable visiblewatermarking,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no.1, pp. 129–133, Jan. 2006.

[6] Y. Hu and B. Jeon, “Reversible visible watermarking and lossless recoveryof original images,” IEEE Trans.

Licensed Under Creative Commons Attribution CC BY

Circuits Syst. Video Technol.,vol. 16, no. 11, pp. 1423–1429, Nov. 2006.

[7] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding—Newparadigm in digital watermarking,” J. Appl. Signal Process., vol. 2002,no. 2, pp. 185–196, Feb. 2002

[8] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spreadspectrum watermarking for multimedia,” IEEE Trans. Image Process.,vol. 6, no. 12, pp. 1673–1687, Jun. 1997.

[9] M. S. Kankanhalli, Rajmohan, and K. R. Ramakrishnan, “Adaptive visiblewatermarking of images,” in Proc. IEEE Int. Conf. MultimediaComputing and Systems, 1999, vol. 1, pp. 568–573.

[10] Y. Hu and S.Kwong,“Wavelet domain adaptive visiblewatermarking,”Electron. Lett., vol. 37, no. 20, pp. 1219–1220, Sep. 2001.

[11] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, “A DCTdomain visible watermarking technique for images,” in Proc. IEEE Int.Conf. Multimedia and Expo, Jul. 2000, vol. 2, pp. 1029–1032.

[12] 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, vol. 2659, pp. 126–133.

[13] 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

[14] International Journal of Computer Applications. Volume 71–No.11, May 2013 40 Design and Implementation of Invisible and Visible Color Image Watermarking with Netbeans IDE ,Baisa L. GunjalAmrutvahini College ofEngineering,Sangamner,Ahmednagar, MS, India. Suresh N. Mali, Principal, Singhgad Institute of Technology and Science, Narhe, Pune, MS, India

[15] International Journal Of Engineering Sciences and management -Generic Lossless Visible watermarkingK.Sundeep, Nellore, P.MunaSwamy, Professor, NEC, Nellore

Licensed Under Creative Commons Attribution CC BY