Asian Journal of Information Technology 6 (5): 607-613, 2007


# Quality Improvement of Digital Watermarking Images

Akram M. Zeki, Azizah A. Manaf and Sayuthi Jaafar
Faculty of Computer Science and Information System, University Technology Malaysia, Malaysia

**Abstract:** In a digital image watermarking system, information carrying watermark is embedded in an image. The most important requirement of watermarking system is the quality of watermarked image. In most applications, the watermarking algorithm must embed the watermark such that this does not affect the quality of the underlying host data. Although many watermarking techniques have been proposed by various researchers, the specific requirements of each watermarking technique vary with the used application. One of the most famous techniques inserts the watermark in the underused Least Significant Bits of the image (LSB). The aim of this study is to improve LSB technique to give better image quality of watermarked images by moving the watermarked pixel to be very close to the original pixel. So in case the hidden bit is not the same as the original bit, the best watermarked image quality will be obtained by moving the pixel to be located in the edge of ranges towards the original pixel.

**Key words:** Watermarking, image quality, bit-planes, LSB, original pixel, digital

## INTRODUCTION

Nowadays, digital watermarking has become a significant topic of computer science due to the increasing popularity of the Internet and the essential need of data security (Chang *et al*., 2004). Digital watermarking technique is a solution to the copyright protection problem of digital media. In addition to copyright protection, digital watermark has various other applications, such as: Fingerprinting, data hiding, authentication and integrity verification, ownership assertion, content labelling, usage control and many other applications. Image watermarking can be classified as visible or invisible. A visible watermarking typically contains a visual message or a company logo indicating ownership of the image. An invisible watermarked image is visually very similar but not necessarily identical to the original unmarked image. Visible watermarking has been dealt with by many researchers, e.g., (Braudaway *et al*., 1996; Berghel, 1997; Yeung *et al*., 1997). Invisible watermarking has received also a good attention, e.g. (Bender *et al*., 1996; Caronni, 1995). The invisible watermark's existence which is going to be used here should be determined only through a watermark extraction or detection algorithm (Yang, 2003).

**Quality of watermarked image:** In most applications, the watermarking algorithm must embed the watermark so that it does not affect the quality of the underlying host data. The watermark is truly imperceptible if humans cannot distinguish the host data from the watermarked data. However, since users of watermarked data normally do not have access to the host data, they cannot perform this comparison. Therefore, it is sufficient that the modifications in the watermarked data go unnoticed as long as the data are not compared with the original data (Kamal, 2003; Shelby, 2000). Perceptual coders minimize the error perceived by the Human Visual System (HVS). This was introduced since it was found that working with the Peak Signal to Noise Ratio (PSNR) criterion and the Mean Square Error (MSE) criteria were inadequate in reducing perceived distortions introduced by compression (Shelby, 2000). The mean squared error MSE is as shown in Eq. 1, which is the averaged term-by-term squared difference between the input signal (the original image, P) and the output signal (the watermarked image, P`). The signal to noise ratio is as shown in Eq. 2, which represents the size of the error relative to the input signal.

$$MSN = \frac{1}{N}\sum^{N}(P_i' - P_i)^2 \quad (1)$$

$$SNR = \frac{\frac{1}{N}\sum_{i}^{N} P_i^2}{MSN} \quad (2)$$

Signal to noise ratio is in decibels units as given by Eq. 3.

$$SNR\ (db) = 10\log_{10} SNR \quad (3)$$

**Corresponding Author:** Akram M. Zeki, B-8-7, Block B, Tasik Heights Apartments, Bandar Tasik Selatan, 57000, Kuala Lumpur, Malaysia

$$PSNR(db) = 10\log10 \frac{P_{peak}^2}{MSN} \quad (4)$$

The Peak Signal to Noise Ratio (PSNR) is given by Eq. 4, where $P_{peak}$ is the peak value of the input signal (usually 255 for 8 bit grey scale images) (Joachim *et al*., 2000; Stefan *et al*., 2002). PSNR has been used to evaluate the quality of watermarked image after embedding the logo. There is no standard value for PSNR but the larger the PSNR give the better the image quality, some research consider undetected image if the PSNR is greater than 30 (Wu, 2004; Bennour *et al*., 2007) while some others asked for 34 db (Cheung, 2000; Eggers *et al*., 2000) and others asked for 38 db for undetected images (Hosinger and Rabbani, 2000; Sun *et al*., 2006).

## WATERMARKING TECHNIQUES

In general, watermark can be embedded in spatial domain or transform domain of an image. In the spatial domain approach, the pixel value of an image is modified to embed watermark information. The spatial techniques insert the watermark in the underused least significant bits of the image. This allows a watermark to be inserted in an image without affecting the value of the image (Zeki *et al*., 2005; Chen, 1999). The simplest example of a spatial domain watermarking techniques to insert data into digital signals in noise-free environments is Least Significant Bit (LSB) coding. For penetrating an image, the grey-scale of each pixel is decomposed into its 8 different bits. The plane formed by the same bit of each pixel in a grey-scale image is called a bit-plane. Figure 1 shows the host image in grey scale level and Fig. 2 shows the eight corresponding bit-planes of Fig. 1. The 1st bit-plane in top left image shows the Most Significant Bits (MSB) while the 8th bit-plane in the button right image shows the Least Significant Bits (LSB). Observing these bit-planes, we can see that some areas in the sixth, seventh and eighth least significant bit planes are bestrewn with noise.

An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding, based on a given key. Security of the watermark would be improved as the

Fig. 1: Grey scale host image

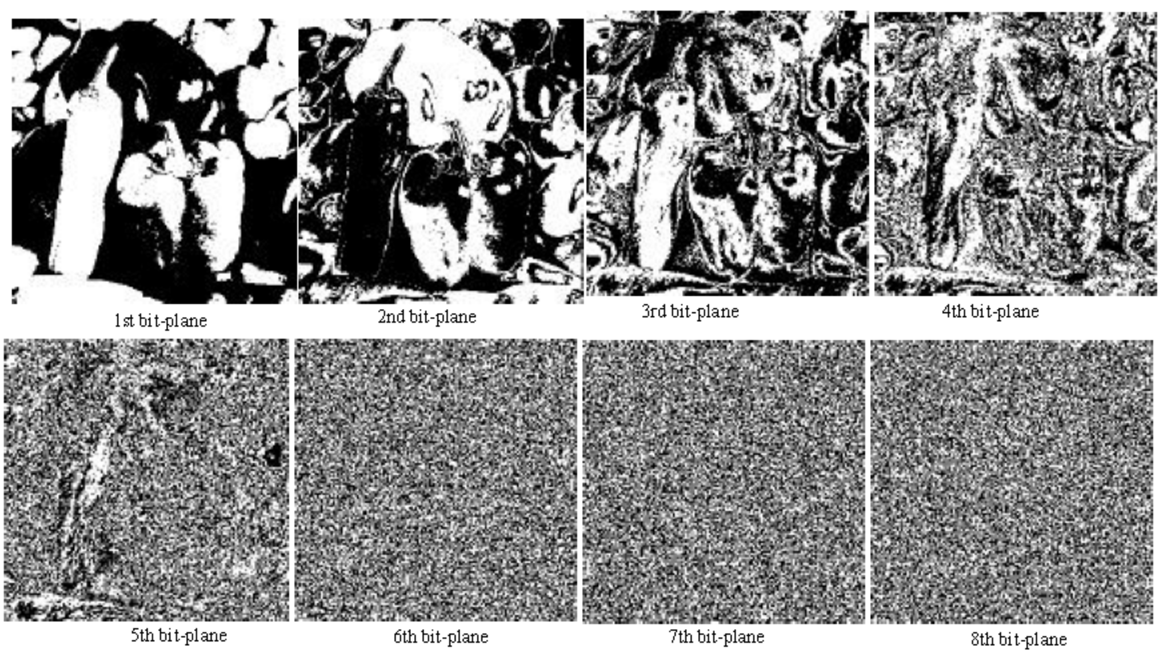


Fig. 2: Eight bit-planes from most significant to least significant bits

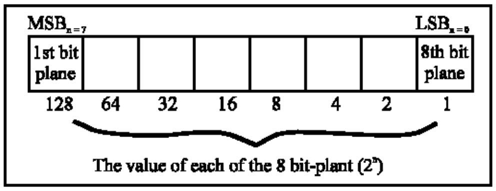


Fig. 3: Eight bit-plane from MSB to LSB

watermark could no longer be easily viewed by intermediate parties. Schyndel *et al.* (1994) proposed a method based on bit plane manipulation of the Least Significant Bit (LSB) which offers easy and rapid decoding. Macq and Quisquater (1995) inserts the watermark into LSB only around image contours. Caronni (1995) hides small geometric patterns called tags in regions where the tags would be least visible, such as the very bright, very dark or texture regions. Bender *et al.* (1996) chooses random pairs of image points and increases the brightness of one and decreases that of the other. Nikolaidis and Pitas (1996) adds a small positive number to random locations as specified by the binary watermark pattern and uses statistical hypothesis testing to detect the presence of watermark. Voyatzis and Pitas (1996) uses dynamic systems to generate chaotic orbits which are dense in the spatial domain and hide the watermark at the seemingly chaotic locations.

## MATERIALS AND METHODS

In this study we improved the direct embedding method (LSB technique) to give better image quality of watermarked image. In grey-scale images which contain 8 bits per pixel, the direct embedding method can be applied in any of these 8 bit planes or may be in more than one plane. While embedding watermark within the 8th bit-plane (Least significant bits) gives best image quality, embedding within the 1st bit-plane (Most significant bits) gives worst image quality. The quality of watermarked image will be improved by embedding when starting from 1st bit-plane to 8th bit-plane (Manef *et al.*, 2006).

In this study one bit-plane only has been selecting to host the watermark, that means the capacity of watermark embedding is 1/8 (12.5% from the original image). The value of each bit of 8 bit-plane can be presented by $2^n$, where n is order of the plane starting from 0 to 7 as shown in Fig. 3. i.e: $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 = 255$. The maximum value that can fit in 8 bits is 255 and minimum value is 0. Any modification to 8th bit-plane will change the pixel value by ±1, while in the 7th bit-plane it will be changed by ±2, the 6th bit-plane by ±4, the 5th bit-plane by ±8, the 4th bit-plane by ±16, the 3rd bit-plane by ±32, the 2nd bit-plane by ±64 and the 1st bit-plane by ±128. As a result if the changed value is small (such as 8th bite-plane) the quality of the image will be good. While a big changed value (such as 1st bit-plane) causes the image quality to be highly distorted.

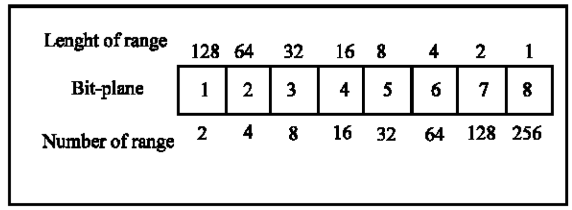


Fig. 4: Eight bit-planes with the number and the length of ranges

After selecting one plane from the 8 bit-planes for hosting the data, the embedding process will be done by inserting the bits of watermark object within the selected bit-plane of the cover image. In order to improve the quality of watermarked image, the other 7 bits will be changed to be very close to the original pixel, that means no changing to the other 7 bits if the hidden bit is the same as the original bit (embedding 1 if the original value was 1, or embedding 0 if the original value was 0). But if the original value is not the same as the embedded one, the nearest pixel to the original will be chosen as a watermarked and this is done by finding a range of the selected bit-plane, the length of the range (L) is $2^n$ and the number of ranges (N) are 256/L. We can notice that in each range the bit changes between 0 and 1.

The number of ranges for the 1st bit-plane are 2 only as follows (0:127) and (128:255). In other words, the bit in the first range is 0, while the bit in the second range is 1 and the length of each range of the first bit-plane is 128. For the second bit-plane there are four range as follows: (0:63) (64:127) (128:191) (192:255) and the length of the ranges is 64 and so on, as shown in Fig. 4.

In the next step of the proposed method, each range will be divided into 2 equal groups. If the original bit is same as the watermark bit, the pixel will not be changed. While if the original bit differs from the watermark bit and the original pixel was in the right group, the watermarked pixel will be the minimum of the next range. Whereas in case the original pixel is in the left group, the watermarked pixel will be the maximum of the previous range as shown in Fig. 5. The proposed method can be presented by few steps as following:

- Selecting one bit-plane from 0 to 8.
- Finding the length of the range of the selected bit-plane by $L = 2^n$ (n for 1st bit-plane is 7 while for 8th bit-plane is 0)

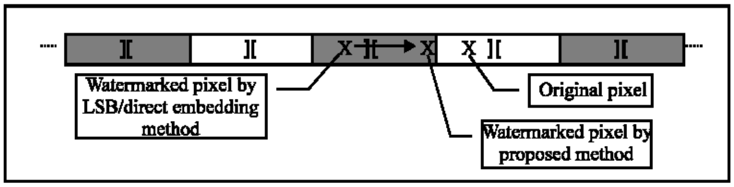


Fig. 5: Proposed method for best watermarked image quality

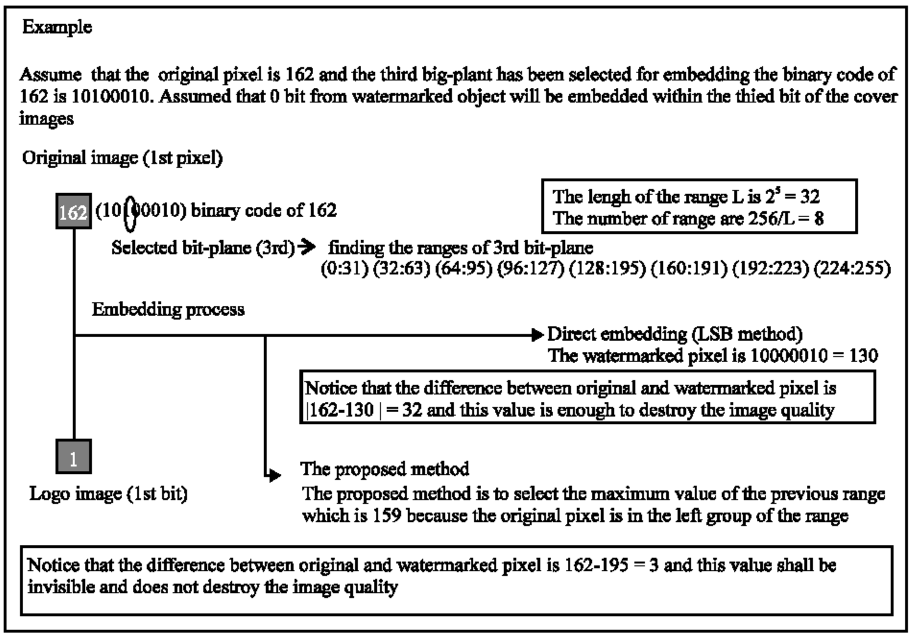


Fig. 6: The details of embedding example by the proposed method

- Arranging table of the ranges for the selected bit-plane (and the number of ranges (N) are 256/L).
- If the original bit is same as the watermark bit, the pixel will not be changed.
- While if the original bit is different than the watermark bit, the other 7 bits will be changed to be very close to the original pixel by the following:
- Each range will be divided into two equal groups: If the original pixel is in the left group, the watermarked pixel will be the maximum of the previous range.
- While if the original pixel is in the right group, the watermarked pixel will be the minimum of the next range.
- If the original pixel is in the first range (no matter if it is in the left or right group), the watermarked pixel will be the minimum of the next range.
- If the original pixel is in the last range (no matter if it is in the left or right group), the watermarked pixel will be the maximum of the previous range.

Figure 6 shows the details of embedding example by the proposed method.

Fig. 7: Grey scale logo with 90×90 pixels

## RESULTS

The logo of University Technology Malaysia which is in grey scale level image and is shown in Fig. 7 contains 90×90 pixels and will be embedded within the host grey scale level images which they are shown in Fig. 8 and containing 256×256 pixels.

The watermark logo has been embedded within all bit-planes of the host images starting from 1st bit-plane (the most significant bits-MSB) through to 8th bit-plane (the last significant bits-LSB). Figure 9 shows the watermarked images after embedding the watermark within all bit-planes by the proposed method and the direct embedding method (LSB technique) for the 3 images.


Fig. 8: Grey scale host images with 256×256 pixels

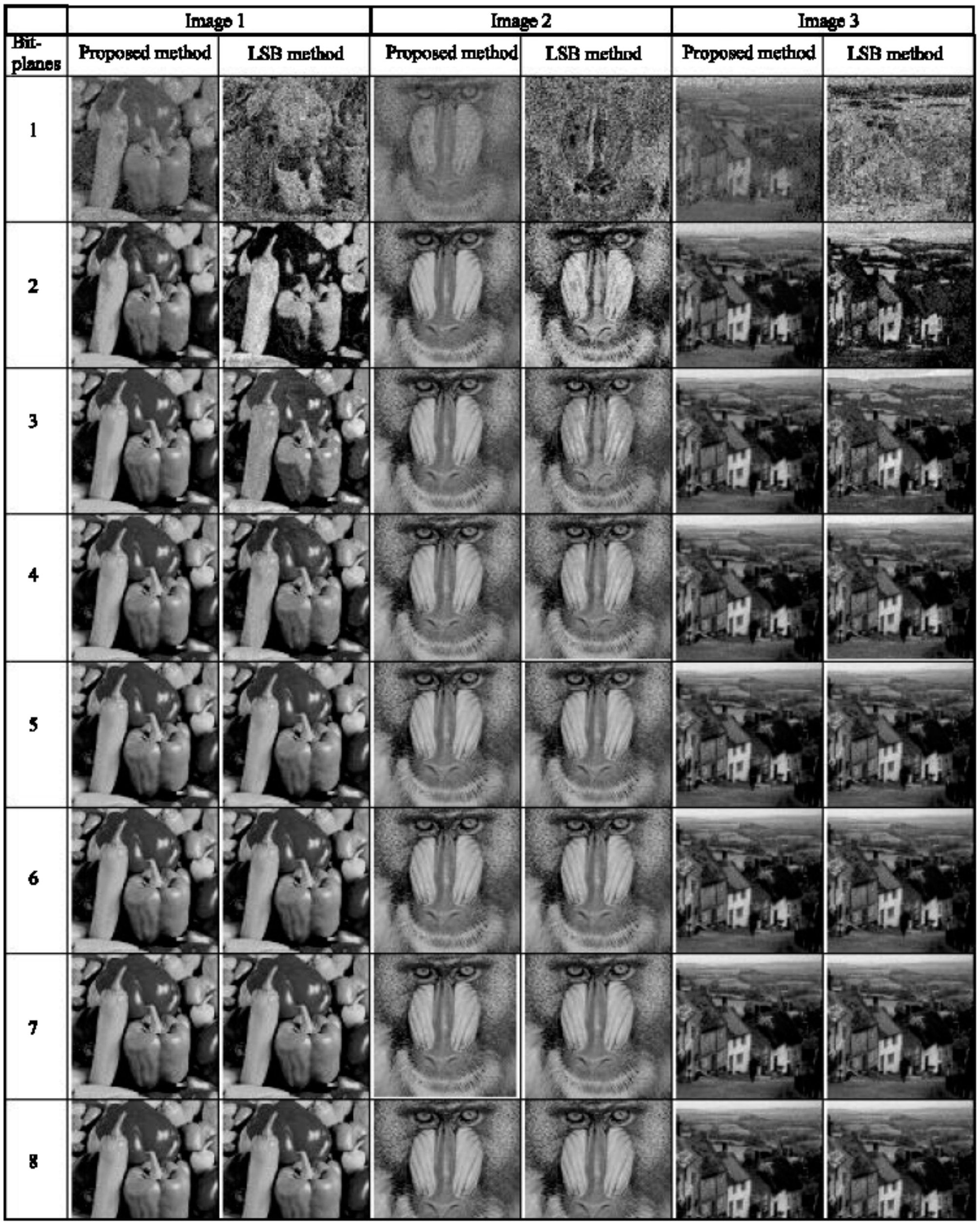


Fig. 9: The watermarked images and PSNR value of the proposed method and LSB method for different bit-planes

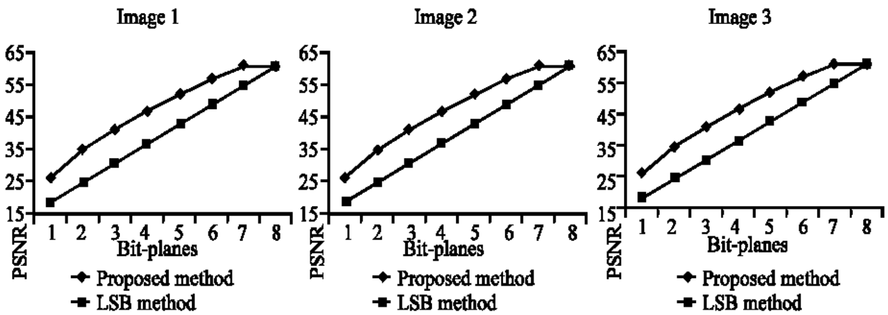


Fig. 10: PSNR value of the proposed method and LSB method for different bit-planes

Table 1: The PSNR value of the proposed method and LSB method for all bit-planes

| | Image 1 | | Image 2 | | Image 3 | |
|---|---|---|---|---|---|---|
| Bit-planes | Proposed method | LSB method | Proposed method | LSB method | Proposed method | LSB method |
| 1 | 26.0280 | 18.3721 | 28.6401 | 18.5807 | 26.4771 | 18.5819 |
| 2 | 33.4937 | 24.1894 | 35.7984 | 24.6016 | 34.7665 | 24.6105 |
| 3 | 40.7375 | 30.3686 | 41.2107 | 30.6495 | 41.0660 | 30.6169 |
| 4 | 46.7111 | 36.7304 | 46.7148 | 36.6602 | 46.5932 | 36.6491 |
| 5 | 51.9437 | 42.6917 | 51.9605 | 42.6702 | 51.9931 | 42.6723 |
| 6 | 56.7520 | 48.6912 | 56.7761 | 48.7020 | 56.7523 | 48.6989 |
| 7 | 60.7245 | 54.7109 | 60.7083 | 54.6877 | 60.7192 | 54.7090 |
| 8 | 60.7473 | 60.7511 | 60.7278 | 60.7278 | 60.7398 | 60.7398 |

The peak signal to noise ratio PSNR has been calculated for each embedding and shown in Table 1. The results of each image have been illustrated in one paragraph in order to compare the proposed method with the LSB method as shown in Fig. 10.

From the above results, we can notice that for 8th bit-plane (least significant bits) the quality has not been improved nor affected by using this method because the length of the range is 1 so the watermarked pixel has no other choice to move in the range and this value is already considered the nearest value to the original pixel value. While for the other bit-ranges the quality of watermarked images has been improved, for example in the 7th bit-plane by direct embedding/LSB method the difference between the original pixel and the watermarked pixel is ±2 while by using proposed method is ±1. That is why the PSNR value for the 7th bit-plane using the proposed method is almost equal to the 8th bit-plane's value.

## CONCLUSION

In general, watermark can be embedded in spatial domain or transform domain of an image. In the spatial domain approach, the pixel value of an image is modified to embed watermark information. In this study, a grey scale logo has been embedded within host grey scale image by proposing a method that improves direct embedding/LSB method. The Peak Signal to Noise Ratio (PSNR) has been used to evaluate the quality of watermarked image. The results show that the quality of watermarked images has been improved by using the proposed method for all bit-planes except the 8th bit-plane. As a future work, more than one watermarked object need to be embedded, the robustness of the proposed technique has to be tested and finding best bit-plane for embedded watermark.

## ACKNOWLEDGEMENT

We would like to thank Malaysian government for sponsoring this research under IRPA grant number: 7424904.

## REFERENCES

Braudaway, G.W., K.A. Magerlein and F.C. Mintzer, 1996. Protecting Publicly Available Images with a Visible Image Watermark. Proc. SPIE Conf. Optical Security and Counterfiet Deterrence Technique, pp: 126-132.

Berghel, H., 1997. Watermarking Cyberspace. Commun. ACM., pp:19-24.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for Data Hiding. IBM Sys. J., pp: 313-336.

Bennour, J., J.L. Dugelay and F. Matta, 2007. Watermarking Attack: BOWS contest. Proceeding of SPIE.

Cheung, W.N., 2000. Digital image watermarking in spatial and transform domains. TENCON. Proceedings, pp: 374-378.

Caronni, G., 1995. Assuring Ownership Rights for Digital Images. Proceeding of Reliable IT. Systems, VIS '95, Vieweg, Germany, pp: 251-265.

Chang, G.M. G.M. Chen and M.H. Lin, 2004. Information hiding based on search-order coding for VQ indices. Pattern Recognition Letters, Vol. 25.

Chen, Pie-Chun 1999. On the Study of Watermarking Application in WWW-Modelling, Performance Analysis and Applications of Digital Image Watermarking Systems. PhD Thesis, Monash University.

Eggers, J.J., Su J.K. and B. Girod, 2000. Robustness of a Blind Image Watermarking Scheme. International Conference on Image Processing ICIP Canada.

Hosinger, C. and M. Rabbani, 2000. Data embedding using phase dispersion. Presented at International Conference on Information Technology: Coding and Computing.

Joachim, J., J. Eggers and G. Bernd, 2000. Robustness of a blind image watermarking scheme. ICIP Special Session on WM, Canada.

Kamal, Gulati, 2003. Information Hiding Using Fractal Encoding. Master thesis, Indian Institute of Technology Bombay, Mumbai.

Manaf, A.A., A.M. Zeki, S. Jaafar and M. Shahidan, 2006. A Secure Digital Watermarking: An Overview. Malaysian Science and Technology Congress (MSTC 2006). Kuala Lumpur, Malaysia, pp: 225-229.

Macq, B.M. and J.J. Quisquater, 1995. Cryptology for Digital TV Broadcasting. Proc. IEEE., 83: 944-957.

Nikolaidis, N. and I. Pitas, 1996. Copyright Protection of Images using Robust Digital Signatures. Proceeding of the IEEE. International Conference on Acoustics, Speech, Signal Processing, 4: 2168-2171.

Shelby, P., 2000. Robust Digital Image Watermarking. PhD Thesis, University of Geneve, Faculty of Science, Canada.

Stefan, W., D. Elisa and T. Gelasca, 2002. Perceptual quality assessment for video watermarking. In: Proc. International Conference on Information Technology: Coding and Computing (ITCC), Las Vegas, NV, pp: 90-94.

Schyndel, R.G. A.Z. Tirkel and C.F. Osborne, 1994. A Digital Watermark. Proc. IEEE International Conference on Image Processing, ICIP-94, 2: 86-90.

Sun, Q., Z. Zhang and D. He, 2006. A Standardized JPEG2000 Image Authentication Solution based on Digital Signature and Watermarking.. Feature Articles: Multimedia Communications. China Communications.

Voyatzis, G. and I. Pitas, 1996. Applications of Toral Automorphisms in Image Watermarking. Proc. IEEE Int. Conf. Image Processing, 2: 237-240.

Wu, N., 2004. A Study on Data Hiding for Gray-Level and Binary Images. Master thesis, Chaoyang University of Technology, Taiwan.

Yeung, M.M., F.C. Mintzer, G.W. Braudaway and A.R. Rao, 1997. Digital Watermarking for High-quality Imaging. Proceedings of 1997 IEEE First Workshop on Multimedia Signal Processing, pp: 357-362.

Yang, Z., 2003. Dual Domain Semi-fragile Watermarking for Image Authentication. Master Thesis, University of Toronto, Canada.

Zeki, A.M., A.A. Manaf and M.Z. Khedher, 2005. Digital Watermarking Embedding in Handwritten Text Images. International Conference on Robotics, Vision, Information and Signal Processing (ROVISP) IEEE., Penang, Malaysia, pp: 618-622.