A New Marginal Color Image Water Marking Method based on Logical Operators

B. Vijaya Kumar[1] M.Radhika Mani[2] G. Roseline NesaKumari[3] and
Dr. V. Vijaya Kumar[4]
[1]Professor& HOD, Dept. of CSE, Lords Inst. of Technology, Hyderabad, A.P., India
[2]Asst. Professor, Dept. of CSE, GIET, Rajahmundry, A.P., India
[3]Assoc. Prof., Dept. of MCA, GIET, Rajahmundry , A.P., India
[4]Dean and Professor, Dept. of CSE and IT, GIET, Rajahmundry, A.P., India
busireddy100@gmail.com[1], sureshaudimulapu@yahoo.com[2],
rosemaruthu@gmail.com [3] , vakulabharanam@hotmail.com[4]

Abstract

Image hiding is a technique that embeds the images into a cover image which makes the watermarks imperceptible so that they can be securely transmitted to the receiver. In this paper, an effective color image watermarking method based on the marginal strategy is proposed. The method uses logical operators like AND and XOR on the nibble to hide the image with in the cover image. To test the robustness of the stego image the present method is applied on different kinds of cover images and the resulting perceptual quality is good.

Keywords: *RGB model, Nibble, distortion, AND operator, XOR operator.*

1. Introduction

Digital content is now posing formidable challenges to content developers, aggregators, distributors and users. The destruction, extraction or modification of the embedded message is required to develop more robust systems so that the digital content processing and organization becomes easy. The shift from cryptography to watermarking because of concealment of image existence as watermarked images which enable to embed the watermark on cover images. Watermarking conceptually implies that the watermark to be transmitted is not visible to the naked eye. Watermarking is used for thousands of years to transmit data without being intercepted by unwanted viewers. It is an art of hiding one information inside another. The main objective of Watermarking is mainly the protection of the contents of hidden information. Images are ideal for hiding information [1, 2] because of the large amount of redundant space is created to store images. Watermarking consists of methods of transmitting secret messages. These secret messages are transferred through unknown cover carriers in such a manner that the very existence of the embedded messages is undetectable. Carriers include images; audio, video, text, or any other digitally represented code or transmission. The hidden message may be plaintext, cipher text, or anything that can be represented as a bit stream.

A famous example of watermarking is "prisoner's problems" [3] where, two prisoners A and B wish to escape from the jail and their cellars are far apart. The only mode of communication is sending messages through the prison officer. Before they are arrested, they agreed upon a watermarking system that describes the way how the secret message is embedded into the cover text. If the prison officer detects conspiracy, the security will be further tightened. The prison officer can deliberately modify the watermarked text to foil the prisoners' escape. In modern image watermarking which exploits the advantages of the present day digital media, the earlier examples appear simple but the concepts are similar. This is largely due to the fact that, multimedia objects generally permits the addition of significantly large amount of payload by means of simple modifications that preserve the perceptual content of the underlying cover image. Hence multimedia objects were found to be perfect to be used as cover messages [4].

Some of the well-known watermarking methods are LSB, Masking and Filtering and Transform techniques. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) [5] of the cover image with the Most Significant Bits (MSB) of the image to be hidden without destroying the statistical property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. In masking and filtering techniques two signals are embedded into each other in such a manner that only one of the signals is perceptible to the human eye. This is mainly used in watermarking techniques. In the transform based method, the spatial domain is transformed into frequency domain using DCT [6], Fast Fourier Transforms (FFT) and Wavelets etc., [7].

A more challenging problem is to hide an image in another image in such a manner that there should be no color distortion in the resultant watermarked image. The reason is that changing a pixel can be easily detected. In this paper, we propose a new scheme that is proved to be more difficult to break than the spatial domain techniques. In the watermarking the measure of watermarked image quality is the most important concept. If the resultant image after embedding the hidden data also remains same as the original image, then that image is more suitable for the transfer of the hidden data. So we need to choose the images which have the appropriate value for various measures. The present paper has used various quality measures of image like MSE, MAE, RMSE, PSNR, SNR, and RSNR. The rest of the paper is organized as follows. Section 2 deals with the proposed methodology for the new watermarking method, Section 3 deals with the results, discussions and the final section deals with conclusions.

2. Methodology

Many research scholars working in the area of color images proposed many watermarking algorithms based on the spatial domain. Generally speaking, human eye are more sensitive to the change in color images than gray-scale images. A little color distortion (even with a higher PSNR value) could be apparently appeared on resulting mixed images. To develop a data-hiding method which has good performance in color images, the use of various logical operators on the lowest nibble of the pixel is employed into the proposed method. In the proposed method the hidden image is first split into three parts, namely Red (R), Green (G) and Blue (B) components. Then each component of the hidden image is embedded in the RGB components of the cover image by using various logical operators on the lowest nibble of the selected pixel. The processing of splitting the image into three components and then processing the three parts individually is called “marginal strategy”. The present paper uses two logical operators called bitAND and bitXOR. The process of embedding is common to all the three components. The methodology is explained for the single component. The pixel of the hidden image is divided into two nibbles (N1 and N2) as shown in Figure 1. These two nibbles are inserted in the lowest nibbles of the successive pixels of the cover image. To insert into the lowest nibbles, bit AND and bit XOR operators are used to reduce the distortion between the original and resultant values.

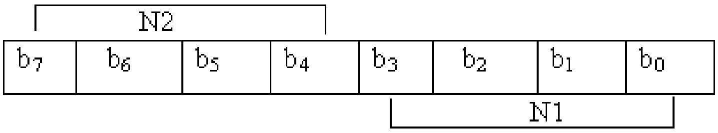

Figure 1. Division of a pixel into two nibbles.

For this, the bitAND operation is performed between the cover image pixel and 240 (11110000). With this, the lowest nibble of the successive pixels (S1 and S2) to 0000. Then perform the bitXOR operation between S1 and N1, S2 and N2. For the reconstruction process, perform the bitAND operation between the watermarked image pixel and 255 (11111111) to extract the lowest nibble. By grouping the successive pixels of the lowest nibble the water marked image can be extracted. The entire process is repeated for the three components (RGB) of the hidden image. The entire process for a single component is shown in the Figure 2. The present paper has used various quality measures of image like Mean Square Error (MSE), Mean Absolute Error (MAE), Root Mean Square Error (RMSE), peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), and Root Signal to Noise Ratio (RSNR) given in Equations (1.1) to (1.6).

$$MAE = \sum_{1}^{M}\sum_{1}^{N}\frac{|I_c - I_s|}{M \times N} \tag{1.1}$$

$$MSE = \sum_{1}^{M}\sum_{1}^{N}\frac{|I_c - I_s|^2}{M \times N} \tag{1.2}$$

$$RMSE = \sqrt{\sum_{1}^{M}\sum_{1}^{N}\frac{|I_c - I_s|^2}{M \times N}} \tag{1.3}$$

$$PSNR = 10 \times \log_{10}\left(\frac{L}{MSE}\right)^2 \tag{1.4}$$

$$SNR = \frac{\sum_{1}^{M}\sum_{1}^{N} I_s{}^2}{\sum_{1}^{M}\sum_{1}^{N}(I_c - I_s)^2} \tag{1.5}$$

$$RSNR = \sqrt{\frac{\sum_{1}^{M}\sum_{1}^{N} I_s{}^2}{\sum_{1}^{M}\sum_{1}^{N}(I_c - I_s)^2}} \tag{1.6}$$

Where I_c is intensity of cover image, I_s is intensity of watermarked image, M×N is the image size and L is the peak signal value of the cover image.

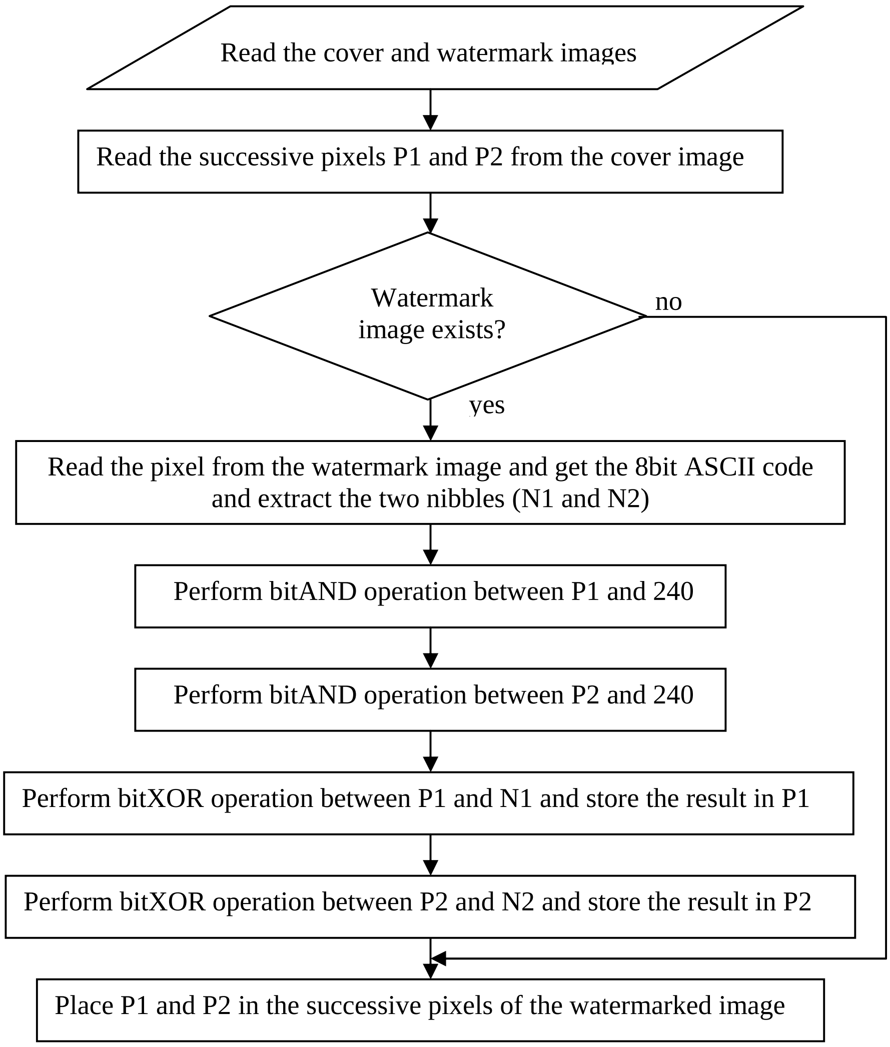

Figure 2. Methodology of the marginal strategy color image watermarking

MAE is the average summation of the absolute difference between the relative positioned pixels of cover & watermarked images. An image that has less MAE value is more preferable for transfer of the secret text, because the noise (I_c-I_s) in the watermarked image will be less. MSE is the average summation of the squares of the difference between the relative positioned pixels of cover & watermarked images. An image that has less MSE value is more preferable for transfer of the secret text. By this minute errors can be detected easily by MSE. RMSE measures the average magnitude of the error. RMSE gives a relatively high weight to large changes in the pixel of the cover image (I_c.-I_s). This means the RMSE is most useful when large changes are present. PSNR is usually expressed in terms of the logarithmic decibel scale. It is the square of ratio of maximum pixel value i.e. 255 to the MSE value. Images having high PSNR value are preferable. For a good image the SNR value must be high, i.e. I_s value present in numerator should be high and I_c-I_s present in the denominator should be low. The RSNR is most useful when large changes are present.

3. Results and Discussions

The proposed method is applied on different cover images of size 256×256. In the present paper, the results are given for four cover images namely leena, Water, Grass and Brick as shown in the figures from 2(a) - 5(a). The bounds of the difference between the cover and watermarked image pixel intensities is ±15 for the three components as the lowest nibble is used to store the hidden image pixel intensity.


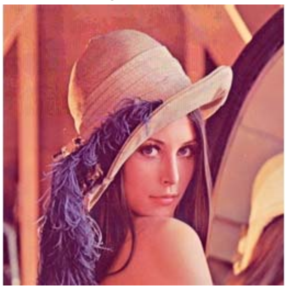


Figure 2(a) Figure 2(b) Figure 2(c)

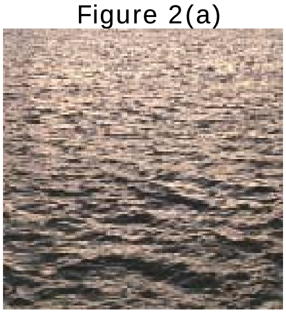

Figure 3(a) Figure 3(b) Figure 3(c)



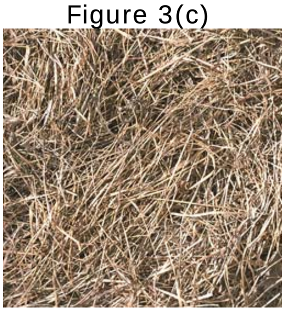

Figure 4(a) Figure 4(b) Figure 4(c)



Figure 5(a) Figure 5(b) Figure 5(c)

Figure 2(a), 3(a), 4(a) and 5(a): Cover Images of Lena, Water.0000, Grass.0002, Brick.0004.

Figure 2(b), 3(b), 4(b) and 5(b): Stego Images for flower hidden image.

Figure 2(c), 3(c), 4(c) and 5(c): Stego Images for human face hidden image.

The watermarks (hidden image) chosen for the present analysis are flower image and human image as shown in the figure 6 and figure 7. The resultant images after inserting the flower and human face image in the cover images of Figure 2(a) to 5(a) are shown in Figure 2(b) to 5(b) and Figure 2(c) to 5(c) respectively.

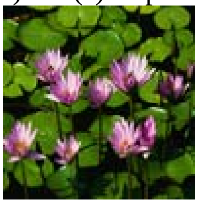

Figure 6. Flower Image Watermark

Figure 7. Human Image Watermark

After completing the entire watermarking process, various quality parameters are estimated and are listed in the Table 1 and Table 2. From the values in Table 1 and Table 2, it can be concluded that the proposed method of watermarking is preferable, since it produces less MSE, MAE, RMSE values and more SNR, PSNR, RSNR values.

Table 1. Estimated Quality Measures of the Cover Images with Flower Image

	MAE	MSE	RMSE	PSNR	SNR	RSNR
Lena	1.2574	23.281	4.825	69.845	101.54	10.077
Water.0000	1.218	21.751	4.6638	71.205	107.1	10.349
Grass.0002	1.2407	22.494	4.7428	70.533	100.57	10.028
Brick.0004	1.2492	22.781	4.7729	70.279	97.037	9.8507

Table 2. Estimated Quality Measures of the Cover Images with Human Image

	MAE	MSE	RMSE	PSNR	SNR	RSNR
Lena	0.98393	14.843	3.8527	78.847	130.32	11.416
Water.0000	0.93658	13.287	3.6451	81.062	139.87	11.826
Grass.0002	0.95739	14.015	3.7437	79.995	130.91	11.442
Brick.0004	0.96835	14.243	3.7739	79.673	125.75	11.214

4. Conclusions

In this paper, a new color image watermarking method is proposed by using logical operators. The watermark image is embedded in all the three components of the cover color image. The results show that the proposed method is imperceptible and has high robustness. The Table 2 indicates the low imperceptibility values for human image watermark when compared to flower image watermark. The greatest advantage of the proposed method is it can hide an image of equal size of cover image.

Acknowledgements

The authors would like to express their cordial thanks to K.V.V. Satya Narayana Raju, Chairman, Chaitanya Institutions and K. Sashi Kiran Varma, Secretary, GIET, Rajahmundry for providing Research facilities. Authors would like to thank Dr. G.V.S. Anantha Lakshmi for her invaluable suggestions and constant encouragement that led to improvise the presentation quality of the paper and Authors would like to thank U.S.N. Raju for his invaluable suggestions.

References

[1] Pfitzmann Birgit, “Information Hiding Terminology”, First International Workshop, Cambridge, UK, Proceedings, Computer Science, 1174, May –June, pp. 347-350.

[2] Westfield Andreas and Andreas Pfitzmann, “Attacks on Steganographic Systems” Third International Workshop, IH'99 Dresden Germany, October Proceedings, Computer Science 1768, 1999, pp. 61- 76.

[3] Niels Provos, “Defending against statistical steganalysis”, In Proceedings of the 10th USENIX Security Symposium, August 2001, pp. 323-335.

[4] R. Anderson and F. Petitcolas, “On the limits of watermarking”, IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998, pp. 474-48 1.

[5] Deshpande Neeta, Kamalapur Snehal, “Implementation of LSB Watermarking and Its Evaluation for Various Bits”, IEEE, 2006.

[6] Constantine Manikopoulos, Yun-Qing Shi, Sui Song, Zheng Zhang, Zhicheng Ni, Dekun Zou, “Detection of block DCT-based Watermarking in gray-scale images”, 2002 IEEE, pp. 355-358.

[7] L.M. Marvel, C.G. Boncelet and C.T. Retter, “Reliable Blind Information Hiding for Images”, In Information Hiding: Second International Workshop, LNCS, Vol. 1525. Springer-Verlag, New York, 1998, pp. 48-61.

Authors

B Vijaya Kumar completed his M S in CSE from DPI, Donetsk, USSR in 1993. He worked as Software Engineer in Serveen Software Systems pvt. Ltd. Secunderabad, India for four years (1993-1997). After that he worked as Sr. Assistant Professor in JBIET, Hyderabad for three years later joined in Royal Institute of Technology & Science, Hyderabad as Associate Professor and worked there for four years. Presently he is working as Professor & Head of CSE Department in Lords Institute of Engineering & Technology, Hyderabad, India. He is pursuing his Ph.D. in Computer Science under the guidance of Dr Vakulabharanam Vijaya Kumar. He is a life member of CSI, ISTE, NESA and ISCA. He has published more than 10 research publications in various National, Inter National conferences, proceedings and Journals.

M. Radhika Mani received the B.Tech (CSE) degree from Sir C.R. Reddy College of Engineering, Andhra University, A.P., India in 2005 and received her M. Tech. (Software Engineering) from Godavari Institute of Engineering and Technology (GIET), JNT University in 2008. Presently she is working as an Assistant Professor in GIET, Rajahmundary. She is pursuing her Ph.D. from JNT University Kakinada in Computer Science. She is a member of SRRF-GIET, Rajahmundry. She has published more than 10 research publications in various National, Inter National conferences, proceedings and Journals.

G Rosline NesaKumari received her M.E., Degree from Sathyabama University Chennai in 2005.She is Pursuing her Ph.D degree in Computer Science and Engineering in Dr MGR University Chennai Under the Guidance of Dr V VijayaKumar Dean & Professor CSE & IT – GIET. She is a life member of Indian Science Congress Association (ISCA). She is now with Godavari Institute of Engineering and Technology as an Associate Professor. Her research interest includes Image processing, Digital Watermarking and Security.

Vakulabharanam Vijaya Kumar received integrated M.S. Engg, degree from Tashkent Polytechnic Institute (USSR) in 1989. He received his Ph.D. degree in Computer Science from Jawaharlal Nehru Technological University (JNTU) in 1998.He has served the JNT University for 13 years as Assistant Professor and Associate Professor and taught courses for M.Tech students. He has been working as Dean for Dept of CSE and IT at GIET, Rajahmundry and Head SRRF-GIET, Affiliated to JNT University Kakinada. His research interests include Image Processing, Pattern Recognition, Network Security, Steganography, Digital Watermarking, and Image retrieval. He is a life member for CSI, ISTE, IE (I), ISCS, IRS, ACS and CS. He has published more than 100 research publications in various National, Inter National conferences, proceedings and Journals.