COMPARISON AND ANALYSIS OF WATERMARKING ALGORITHMS IN COLOR IMAGES – IMAGE SECURITY PARADIGM

D. Biswas[1], S. Biswas[2], P.P. Sarkar[2], D. Sarkar[2], S. Banerjee[1], A. Pal [1]

[1]Academy of Technology, Hoogly – 712121, West Bengal, India.
E-mail: debaindia@rediffmail.com , snehasish_banerjee@ymail.com

[2]USIC, University of Kalyani, Kalyani, Nadia – 741235, West Bengal, India.
E-mail: biswas.su@gmail.com

ABSTRACT

This paper is based on a comparative study between different watermarking techniques such as LSB hiding algorithm, (2, 2) visual cryptography based watermarking for color images [3,4] and Randomized LSB-MSB hiding algorithm [1]. Here, we embed the secret image in a host or original image, by using these bit-wise pixel manipulation algorithms. This is followed by a comparative study of the resultant images through Peak Signal to Noise Ratio (PSNR) calculation. The property wise variation of different types of secret images that are embedded into the host image plays an important role in this context. The calculation of the Peak Signal to Noise Ratio is done for different color levels (red, green, blue) and also for their equivalent gray level images. From the results, we are trying to predict which technique is more suitable to which type of secret image.

KEYWORDS

Steganography, Visual Cryptography, Watermarking, LSB hiding, PSNR

1. Introduction

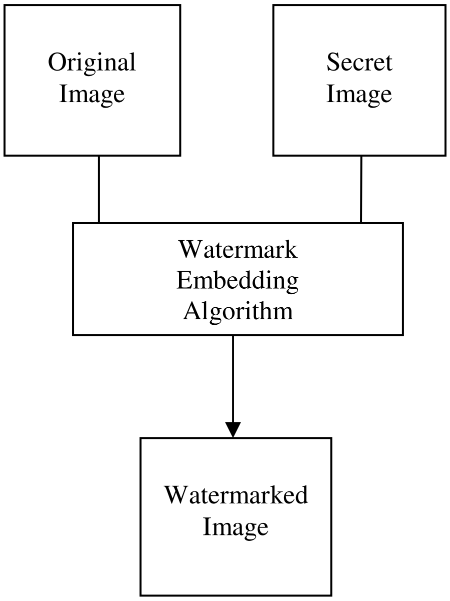
With the growth of the Internet, more and more information is being transmitted in digital format (image, audio, video, etc.) now than ever before. However, the greatest pitfall in transmission of digital information is its easy susceptibility to have innumerable copies of the same nature and quality as that of the original. So, there is always the chance of lack of authentication, ownership proof and copyright protection. So, various steganographic algorithms and embedding techniques have been established to solve this problem that stress on copyright marking. Some message is secretly inserted within the original digital message and that secret message is used to assert copyright over the host digital message. But all such algorithms must satisfy a number of requirements to maintain the quality and integrity of the resultant information. The integrity of the original image must not be changed from the perspective of the human senses. If it becomes perceivable or noticeable, then any third party may see that information is being hidden and therefore may attempt to extract or destroy it. Also it must be resistant to modifications and alterations. Among the different available digital information, we have dealt with images and worked on digital image watermarking. We believe that the different watermarking algorithms on color images have a preference for some particular type of secret image. Their performance is also a function of some parameters of the secret image like brightness, contrast, etc. So here we follow some of the well known

DOI : 10.5121/ijcsit.2011.3303

watermarking techniques and study whether some particular type of secret image is working better for a particular algorithm. In this paper, particularly we have considered two types of secret images – one with greater number of whitish pixels and the other with greater number of darkish pixels. Generally, a secret image is formed on some basic ideas or using some identification marks. A specific pattern can be imposed on the design strategy of those secret images so that it can be very useful in case of digital watermarking. It is worth noting how the same color image watermarking algorithm gives different range of PSNR values for the two different classes of secret images. We are trying to analyze and predict which algorithm scores better for which type of secret images.

2. Related works and fundamentals

Different watermarking algorithms have been introduced from time immemorial. To study the effect of different secret images on the watermarking algorithms, we start with one of the most primitive and well-known algorithms, called the Least Significant Bit (LSB) hiding algorithm. Then, we have used the visual cryptographic watermark method based on Hwang and Naor-Shamir [3, 4] approaches. Two shares are created from the secret image and watermarking is done with one of the shares instead of the actual secret image, to make the approach more robust and immune to attacks. It is to be ensured that the secret message cannot be removed by any attacker without significantly altering the data in which it is embedded. The embedded data must remain confidential unless an attacker can find a way to detect it. So, next we have used the Randomized LSB hiding algorithm [1] (which is extremely difficult to attack) developed by us to test the two types of secret images. The basic block diagram of any standard watermarking algorithm is shown below:



3. Score of LSB hiding algorithm

The classifications of LSB hiding into two separate groups are :

- n LSB-MSB hiding algorithms
- n LSB-LSB hiding algorithms

Where n is the number of bits used.

In LSB-MSB algorithms, the least significant bits of the original image is masked and substituted by the most significant bits of the watermark image. In LSB-LSB algorithms, however, the least significant bits of the original image is masked and substituted by the least significant bits of the watermark image.

It is quite obvious that smaller the value of n, lesser is the deterioration in the quality of the image. As we increase the number of bits, the image quality further degrades and becomes more visible to the naked eye.

3.1 Secret images with less white pixels

Here, the LSB hiding algorithm is applied on some secret images with less white pixels and it is superimposed on the original host image to produce the watermark image.

3.1.1 Experiment 1

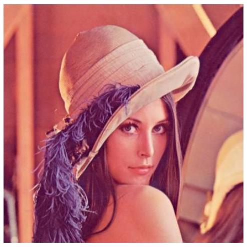


Figure 1: original image

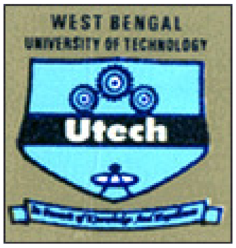


Figure 2: secret image

The output images of n LSB - LSB algorithm :

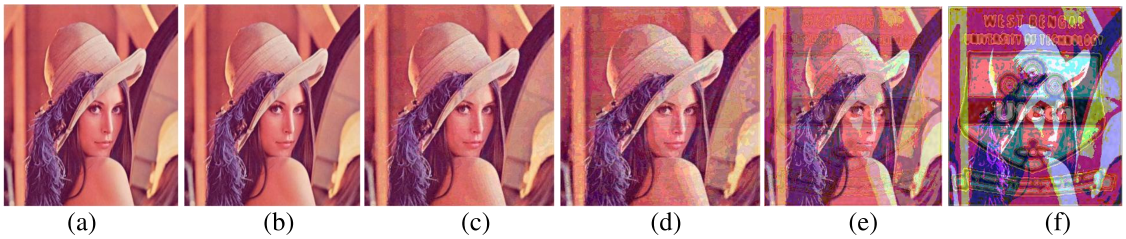


Figure 3: (a) 1 LSB-LSB hiding; (b) 2 LSB-LSB hiding; (c) 4 LSB-LSB hiding; (d) 5 LSB-LSB hiding; (e) 6 LSB-LSB hiding; (f) 7 LSB-LSB hiding.

The output images of n LSB - MSB algorithm :

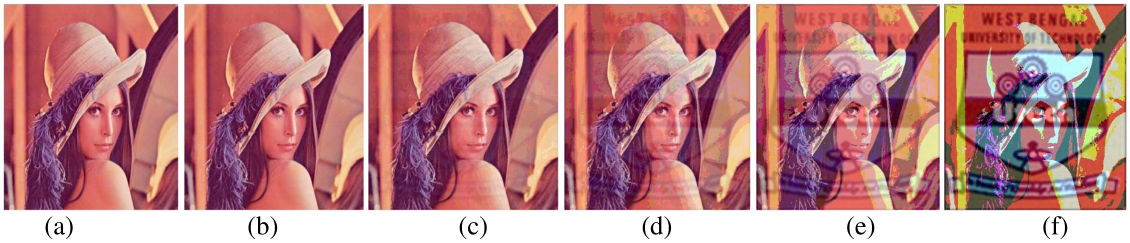


Figure 4: (a) 1 LSB-MSB hiding; (b) 2 LSB-MSB hiding; (c) 4 LSB-MSB hiding; (d) 5 LSB-MSB hiding; (e) 6 LSB-MSB hiding; (f) 7 LSB-MSB hiding.

Peak Signal to Noise Ratio (PSNR) is hugely used in image compression and image modification where the signal is the original data and the noise is the error introduced by compression. For color images, the definition of the PSNR is the same except the Mean Squared Error (MSE) is the sum over all squared value differences divided by image size and by three. When two images are identical, the Mean Squared Error will be zero. So, PSNR will be undefined. It is expressed in logarithmic decibel scale. Here, The calculation of Peak Signal to Noise Ratio is done for different color levels (red R, green G, blue B) and also for their equivalent gray (GY) level images.

Approach	PSNR R	PSNR G	PSNR B	PSNR GY
1 LSB-LSB	37.61	39.74	37.72	41.39
2 LSB-LSB	37.44	39.68	37.73	41.24
3 LSB-LSB	36.97	39.23	37.68	40.62
4 LSB-LSB	34.87	36.72	36.29	37.73
5 LSB-LSB	30.42	31.67	33.68	32.50
6 LSB-LSB	28.92	30.64	31.95	31.21
7 LSB-LSB	25.57	27.66	29.61	26.97

Table 1: PSNR for n LSB-LSB

Approach	PSNR R	PSNR G	PSNR B	PSNR GY
1LSB-MSB	37.55	39.89	37.47	41.48
2LSB-MSB	37.15	39.65	37.56	41.12
3LSB-MSB	36.14	38.72	37.35	39.86
4LSB-MSB	33.51	36.14	35.39	36.51
5LSB-MSB	30.29	31.93	31.72	32.05
6LSB-MSB	28.50	30.06	29.40	30.06
7LSB-MSB	26.12	28.73	26.99	28.10

Table 2: PSNR for n LSB-LSB

3.1.2 Experiment 2

Another secret image with less white pixels is given below in figure 6.

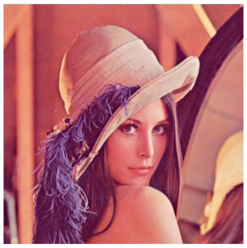


Figure 5: original image

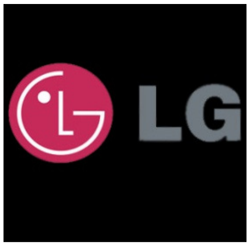


Figure 6: secret image

The output images of n LSB - LSB algorithm :

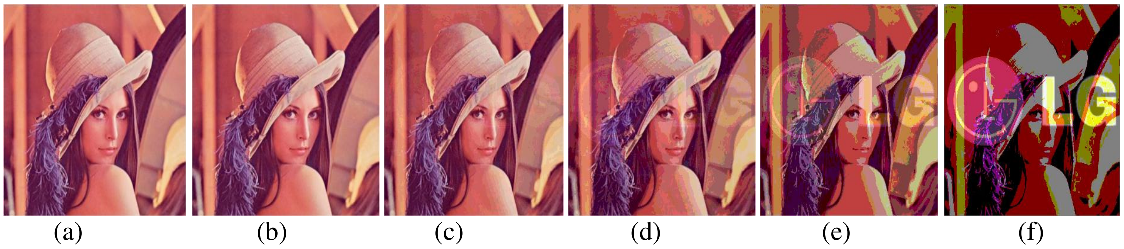


Figure 7: (a) 1 LSB-LSB hiding; (b) 2 LSB-LSB hiding; (c) 4 LSB-LSB hiding; (d) 5 LSB-LSB hiding; (e) 6 LSB-LSB hiding; (f) 7 LSB-LSB hiding.

The output images of n LSB - MSB algorithm :

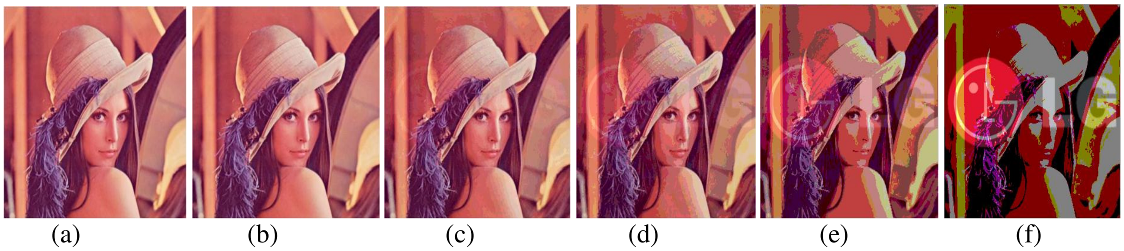


Figure 8: (a) 1 LSB-MSB hiding; (b) 2 LSB-MSB hiding; (c) 4 LSB-MSB hiding; (d) 5 LSB-MSB hiding; (e) 6 LSB-MSB hiding; (f) 7 LSB-MSB hiding.

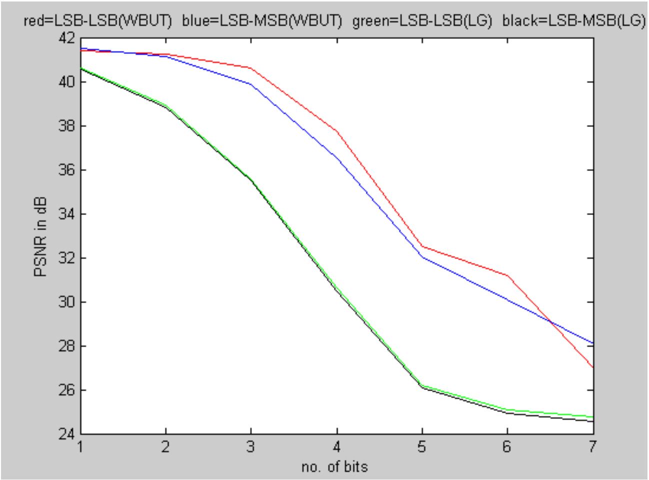


Figure 9: Graph for Experiment 1 and Experiment 2 where secret images are with *less white pixels*

From the above experimental results, it shows that image in which more pixels are of darker colors, LSB-LSB generally gives better result.

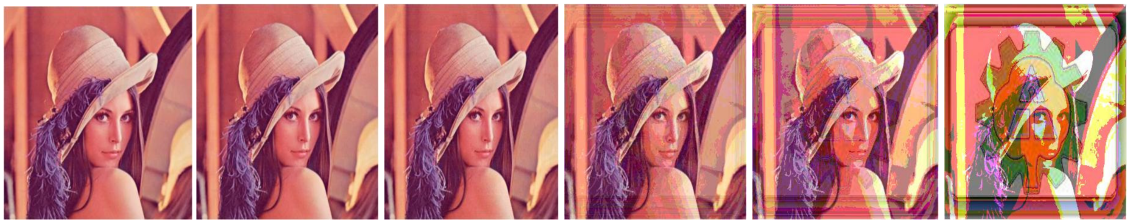
3.2 Secret images with more white pixels

Here, the LSB hiding algorithm is applied on some secret images with more white pixels and it is superimposed on the original host image to produce the watermark image.

3.2.1 Experiment 3

Figure 10: original image Figure 11: secret image

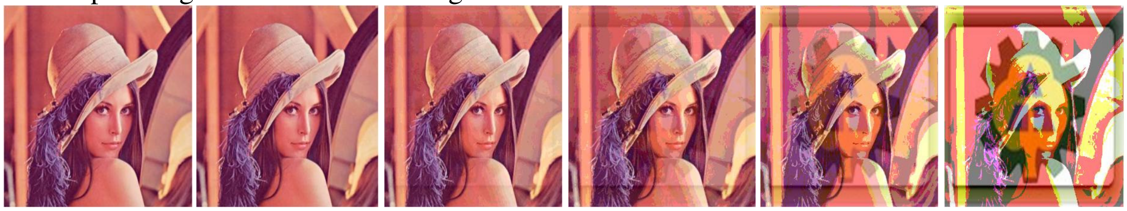
The output images of n LSB - LSB algorithm :



(a) (b) (c) (d) (e) (f)

Figure 12: (a) 1 LSB-LSB hiding; (b) 2 LSB-LSB hiding; (c) 4 LSB-LSB hiding; (d) 5 LSB-LSB hiding; (e) 6 LSB-LSB hiding; (f) 7 LSB-LSB hiding.

The output images of n LSB - MSB algorithm :



(a) (b) (c) (d) (e) (f)

Figure 13 : (a) 1 LSB-MSB hiding; (b) 2 LSB-MSB hiding; (c) 4 LSB-MSB hiding; (d) 5 LSB-MSB hiding; (e) 6 LSB-MSB hiding; (f) 7 LSB-MSB hiding.

3.2.2 Experiment 4

Another secret image with more white pixels is given below in figure 16.

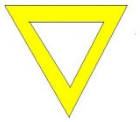


Figure 14: original image Figure 15: secret image

The output images of n LSB - LSB algorithm :

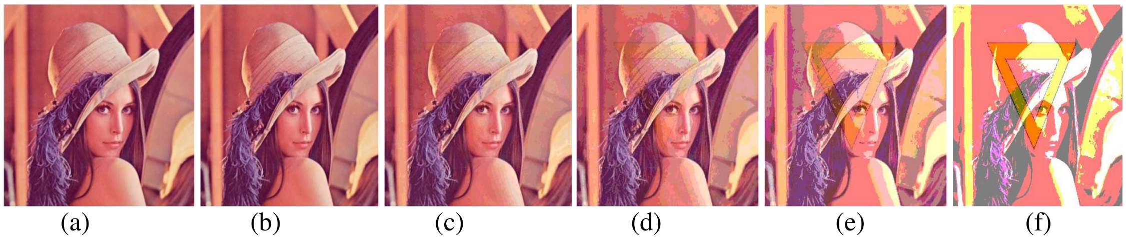

(a) (b) (c) (d) (e) (f)

Figure 16: (a) 1 LSB-LSB hiding; (b) 2 LSB-LSB hiding; (c) 4 LSB-LSB hiding; (d) 5 LSB-LSB hiding; (e) 6 LSB-LSB hiding; (f) 7 LSB-LSB hiding.

The output images of n LSB - MSB algorithm :

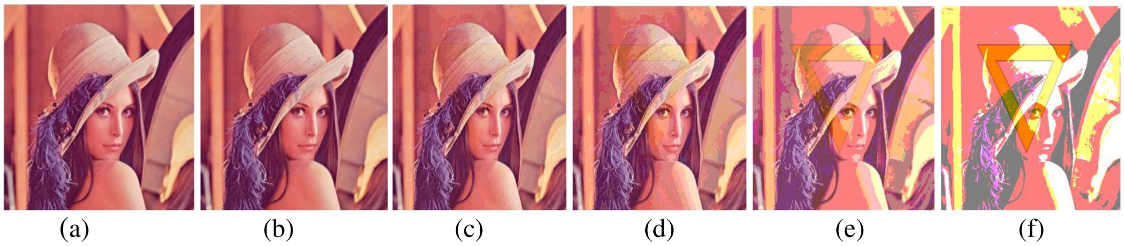

(a) (b) (c) (d) (e) (f)

Figure 17 : (a) 1 LSB-MSB hiding; (b) 2 LSB-MSB hiding; (c) 4 LSB-MSB hiding; (d) 5 LSB-MSB hiding; (e) 6 LSB-MSB hiding; (f) 7 LSB-MSB hiding.

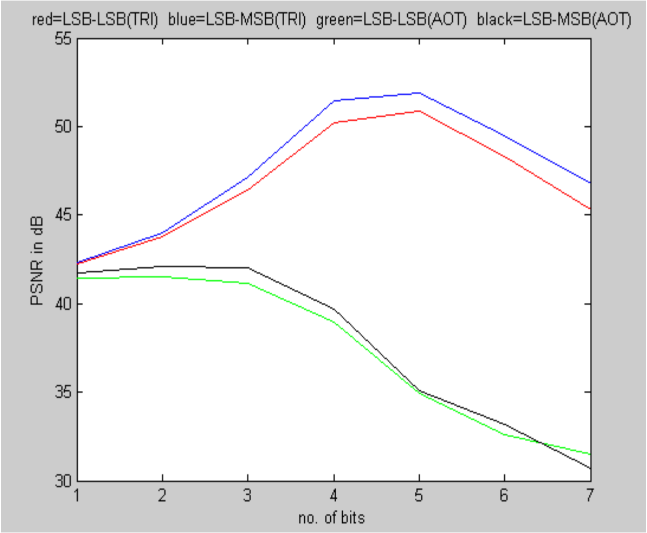
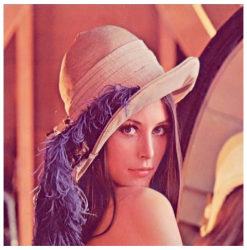


Figure 18: Graph for Experiment 3 and Experiment 4
where secret images are with more white pixels

From the above experimental results, it shows that images in which more pixels are of white colors; LSB-MSB gives better result.

4. Direct LSB hiding algorithm Vs. Visual Cryptography based watermarking

In case of direct LSB hiding algorithm, the secret image is directly embedded with the host image. Where as in Visual Cryptography based watermarking technique, the secret image is split into two shares with the help of (2,2) visual cryptography secret sharing scheme. Then, one of the shares is embedded into the host image and other is held by the owner.



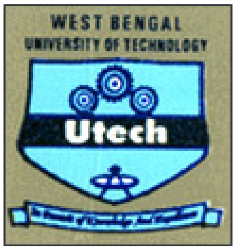
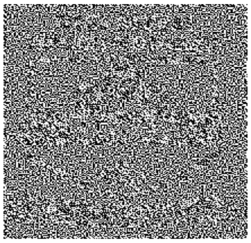


Figure 19: Original image Figure 20: Secret image

Shares of the secret image are as follows:



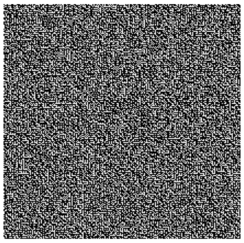


Figure 21: Share 1 image Figure 22: Share 2 image

After merging two shares, we get,

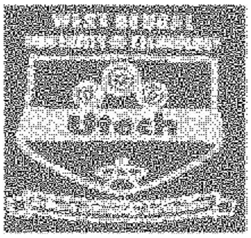


Figure 23: Merged of two shares

The output images of n LSB-LSB algorithm with share1 image of the secret image :

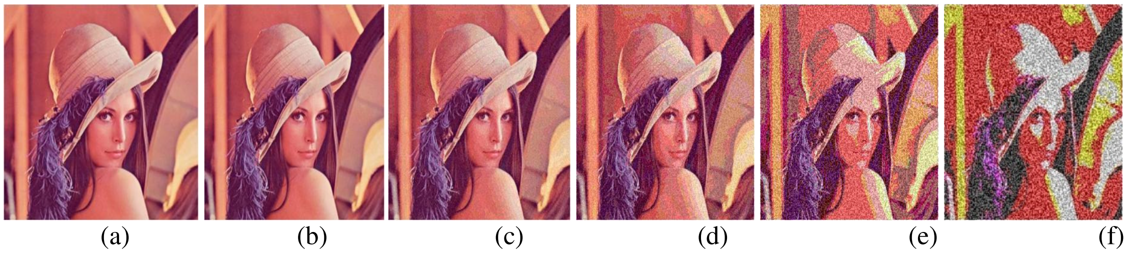
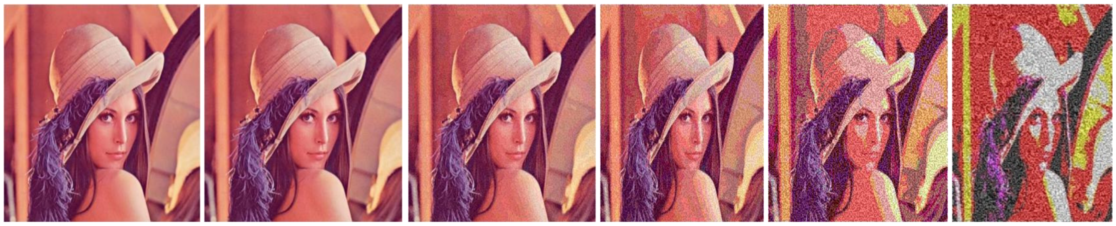


Figure 24: (a) 1 LSB-LSB hiding; (b) 2 LSB-LSB hiding; (c) 4 LSB-LSB hiding; (d) 5 LSB-LSB hiding; (e) 6 LSB-LSB hiding; (f) 7 LSB-LSB hiding.

The output images of n LSB-MSB algorithm with share1 image of the secret image :



(a) (b) (c) (d) (e) (f)

Figure 25 : (a) 1 LSB-MSB hiding; (b) 2 LSB-MSB hiding; (c) 4 LSB-MSB hiding; (d) 5 LSB-MSB hiding; (e) 6 LSB-MSB hiding; (f) 7 LSB-MSB hiding.

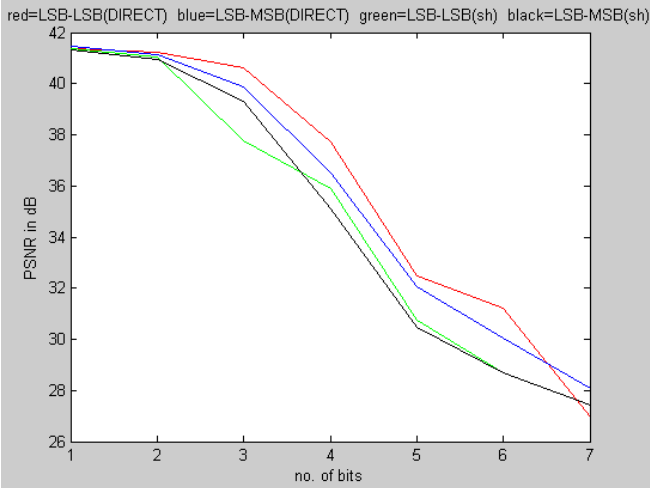


Figure 26: Graph for comparative study of Direct LSB hiding algorithm and Visual Cryptography based watermarking

So, direct LSB hiding watermark algorithm gives more desirable PSNR results than visual cryptography based watermarking (i.e. with shares). So, it will be more useful to embed the secret image directly with the original image rather than embedding one of the shares of the secret image.

5. Score of Randomized LSB (RLSB) hiding algorithm

The algorithm in general, can be represented as Randomized m-n LSB hiding. Here we generate m random numbers that behave as secret keys. Their values are known only to the owner of the image. Here too, we can follow either n LSB-MSB hiding or n LSB-LSB hiding, but we apply them not on all the pixels of the picture but only on some selected pixels whose values are determined by the secret keys. Depending on the 'm' randomly generated values, we can either apply LSB hiding in those particular rows or columns, i.e., either horizontally or vertically. So, the attackers cannot separate the original image unless and until they come to know the values of the secret keys. In this fashion, the time complexity is also greatly reduced rather than other watermarking algorithms.

5.1 Secret image with less white pixels

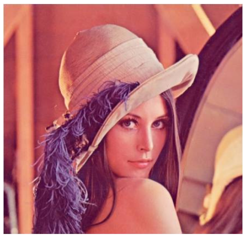


Figure 27: original image

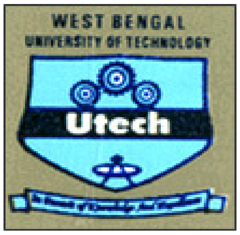
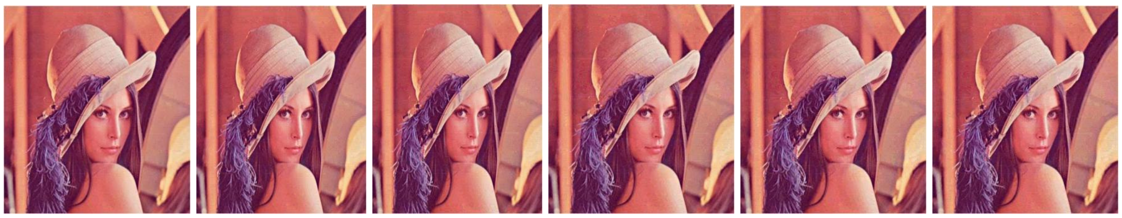


Figure 28: secret image

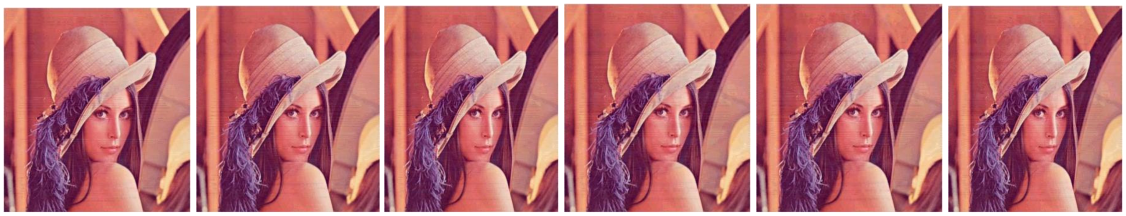
The output images of Randomized m-nLSB – LSB hiding algorithm :



(a) (b) (c) (d) (e) (f)

Figure 29 : (a) Rand.100 – 4LSB–LSB; (b) Rand.120 – 4LSB–LSB; (c) Rand.140 – 4 LSB–LSB; (d) Rand.240 – 4 LSB–LSB; (e) Rand.260 – 4 LSB–LSB; (f) Rand.280 – 4 LSB–LSB.

The output images of Randomized m-nLSB – MSB hiding algorithm:



(a) (b) (c) (d) (e) (f)

Figure 30 : (a) Rand.100 – 4LSB–MSB; (b) Rand.120 – 4LSB–MSB; (c) Rand.140 – 4 LSB–MSB; (d) Rand.240 – 4 LSB–MSB; (e) Rand.260 – 4 LSB–MSB; (f) Rand.280 – 4 LSB–MSB.

LSB-LSB Approach (m)	PSNR	PSNR	PSNR	PSNR
	R	G	B	GY
100	37.02	38.95	37.44	40.38
120	36.86	38.81	37.46	40.16
140	36.76	38.73	37.39	40.06
160	36.67	38.53	37.36	39.88
180	36.54	38.53	37.27	39.65
200	36.28	38.29	37.16	39.46
220	36.29	38.22	37.09	39.35
240	36.13	37.99	37.09	39.18
260	36.08	37.81	37.02	39.04
280	36.02	37.85	36.99	39.03

Table 3: Randomized LSB – LSB with n=4

LSB-MSB Approach (m)	PSNR	PSNR	PSNR	PSNR
	R	G	B	GY
100	36.21	38.47	36.83	39.43
120	36.02	38.23	36.89	39.19
140	35.81	37.99	36.63	38.84
160	35.59	38.04	36.62	38.84
180	35.45	37.68	36.33	38.41
200	35.37	37.86	36.59	38.63
220	35.06	37.38	36.40	38.07
240	35.07	37.52	36.48	38.18
260	35.04	37.49	36.26	38.11
280	34.84	37.30	36.13	37.86

Table 4: Randomized LSB – MSB with n=4

5.2 Secret image with more white pixels

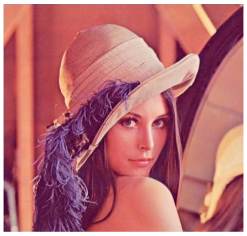


Figure 31: Original image

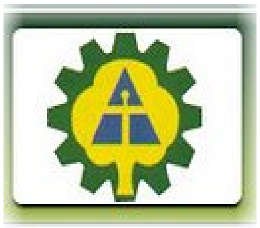
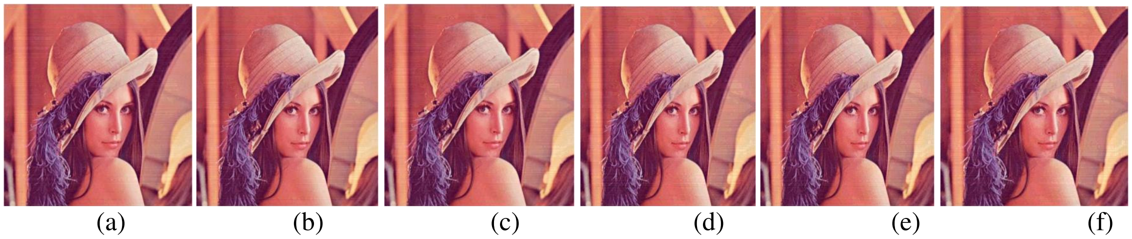


Figure 32: Secret image

The output images of Randomized m-nLSB – LSB hiding algorithm:



(a) (b) (c) (d) (e) (f)

Figure 33 : (a) Rand.100 – 4LSB–LSB; (b) Rand.120 – 4LSB–LSB; (c) Rand.140 – 4 LSB–LSB; (d) Rand.240 – 4 LSB–LSB; (e) Rand.260 – 4 LSB–LSB; (f) Rand.280 – 4 LSB–LSB.

The output images of Randomized m-nLSB – MSB hiding algorithm :

Figure 34 : (a) Rand.100 – 4LSB–MSB; (b) Rand.120 – 4LSB–MSB; (c) Rand.140 – 4 LSB–MSB; (d) Rand.240 – 4 LSB–MSB; (e) Rand.260 – 4 LSB–MSB; (f) Rand.280 – 4 LSB–MSB.

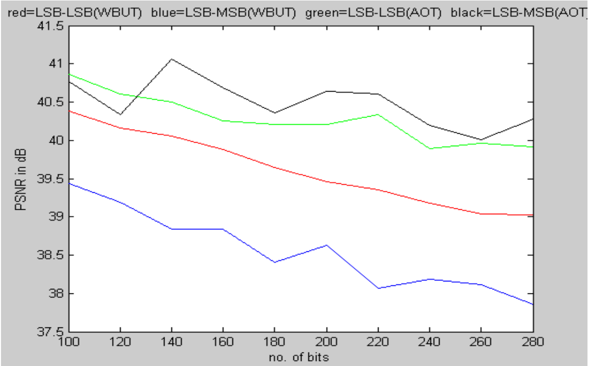


Figure 35: PSNR Graph for secret images used in 4.1 and 4.2 in randomized fashion

So, in case of randomized LSB, there is hardly anything to choose between LSB-LSB and LSB-MSB as both give almost similar PSNR values irrespective of the image type. Moreover, the PSNR is high for any standard value of m as shown in the graph.

6. Conclusions

Through the course of this work, we have analyzed and scrutinized the PSNR values of those embedded images generated by some simple watermark embedding techniques using pixel bit manipulation. It is very difficult to conclude with absolute certainty exactly which watermarking algorithm is the best. This is because the results are very much related to the images that we are embedding.

From the graphs and tables, we can infer that direct LSB hiding watermarking with the secret image gives more desirable PSNR results than visual cryptography based watermarking (with shares).

From the experimental results, it is also certain that the in case of direct watermarking, if the secret image has a higher concentration of white pixels, then LSB-MSB gives better PSNR results. But if more pixels are of darker colors, LSB-LSB gives better results.

For all images PSNR values for VC based watermarking gives almost similar results irrespective of whether the approach is LSB-LSB or LSB-MSB. This is true irrespective of the type of the image because the shares of all images will be more or less similar in pixel composition (only black and white).

For randomized approach, both LSB-LSB and LSB-MSB give almost similar PSNR values irrespective of the image type. Moreover, the PSNR is high for any standard value of m as shown in the graph. It is easy to conclude that among these, Randomized LSB hiding algorithm gives the best result and is most efficient. More specifically, we can say that Randomized m-n LSB-LSB hiding algorithm is better than Randomized m-n LSB-MSB hiding algorithm.

So, direct LSB hiding watermarking is better than VC based watermarking with respect to PSNR values. But direct LSB hiding has the drawbacks of higher complexity and its dependency on the type of the image. This is where randomized LSB scores more than direct LSB hiding as it has lesser complexity and the approach is more robust to variations in image type.

7. References

[1] D. Biswas, S. Biswas, P. P. Sarkar, D. Sarkar, A. Pal, S. Banerjee, S. Polle, F. K. M. Nawaz, K. Das, “Embedding Watermark by Pixel Bit Manipulation”, IEEE conference on Scientific Paradigm Shift in Information Technology and Management (SPSITM), 2011.

[2] G.Langelaar, I. Setyawan, and R. Lagendijk. Watermarking digital image and video data. IEEE Signal Processing Magazine, 17:20–46, 2000.

[3] N.Naor and A.Shamir, “Visual Cryptography”, Advances in cryptology: Eurocrypt’94, Springer-Verlag, Berlin,1995,pp.1-12.

[4] R. J. Hwang, “ A Digital Copyright Protection Scheme Based on Visual Cryptography”, Tamkang Journal of Science and Engineering, vol. 3,no. 3, 2000.

[5] C.Rey and JL.Dugelay. A survey of watermarking algorithms for image authentication. EURASIP Journal on Applied Signal Processing, 6:613–621, 2002.

[6] Gregory Kipper,"Investigator's Guide to Steganography ".

[7] Stefan Katzenbeisser and Fabien, A.P. Petitcolas , "Information Hiding Techniques for Steganography and Digital Watermarking".

[8] Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, 1998.

[9] Niels Provos and Peter Honeyman, University of Michigan, "Hide and Seek: An Introduction to Steganography" IEEE Computer Society IEEE Security & Privacy.

[10] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001.

[11] C. Rafael and E. Richard, Digital Image Processing, Second Edition, Prentice Hall, 2002.

[12] J. Fridrich and M. Goljan, “ Comparing robustness of watermarking techniques”, Proceedings of the SPIE/IS&T Conference on security and watermarking of mult media contents, Vol. 3657, San Josh, CA, Jan. 1999.

[13] Hiding secrets in computer files: steganography is the new invisible ink, as codes stow away on images-An article from: The Futurist by Patrick Tucker.

[14] R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography," IEEE Journal of Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474-481.

[15] Ismail Avcýbas¸, Member, IEEE, Nasir Memon, Member, IEEE, and Bülent Sankur, Member, "Steganalysis Using Image Quality Metrics," IEEE Transactions on Image Processing, Vol 12, No. 2, February 2003.

[16] R. Fisher, K Dawson-Howe, A. Fitzgibbon, C. Robertson, E. Trucco (2005). Dictionary of Computer Vision and Image Processing. John Wiley.

[17] Cox M. Miller and J. Bloom (2001) Digital Watermarking. San Mateo, CA: Morgan Kaufmann.

[18] Diljith M. Thodi and Jeffrey J. Rodríguez (2007) Expansion Embedding Techniques for Reversible Watermarking. IEEE Trans. on Image Processing. 16, (3),721-730.

[19] Fridrich J, Goljan M and Du R (2002) Lossless data embedding new paradigm in digital watermarking.EURASIP J. Appl. Signal Processing, 2002 (2), 185-196.

[20] Ghouti L, Bouridane A, Ibrahim MK and Boussakta (2006) Digital image watermarking using balanced multiwavelets. IEEE Trans. Signal Process. 54 (4), 4707-4719.

[21] Arnold M. Audio watermarking: Features, applications and algorithms. In *IEEE Int. Conf. Multimedia and Expo 2000*, vol. 2, 2000, 1013-1016.

[22] Arnold M. Attacks on digital audio watermarks and countermeasures," in *IEEE Int. Conf. WEB Delivering of Music*, 2003, 1-8.

[23] Bender W., Gruhl D., Morimoto N., Lu A. Techniques for data hiding. *IBM Syst. J.*, vol. 35, no. 3/4, 1996, 313-336.

[24] Ching-Sheng Hsu, Shu-Fen Tu, "Digital Watermarking Scheme with Visual Cryptography", Proceedings of the International Multi-Conference of Engineers and Computer Scientists 2008 Vol. I, 19-21 March, 2008, Hong Kong.

[25] Black M., Zeytinoglu M. Computationally efficient wavelet packet coding of wide-band stereo audio signals. In *IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, 1995, 3075-3078.

[26] Kundur D., Hatzinakos D. Toward robust logo watermarking using multiresolution image fusion principles. *IEEE Trans.Multimedia*, vol.6, no.1, 2004, 185-194.

Authors

Mr. Debasish Biswas attained his M.Tech (Computer Science & Engg.) from Calcutta University, India. He is currently an Asstt. Professor in Department of Computer Science & Engg. , Academy of Technology, West Bengal University of Technology, India. His research interests are in the field of Steganography, Visual Cryptography, and image processing.

Dr. Susanta Biswas received Ph.D. degree in Electronics Engineering from Jadavpur University, India. He is currently a Senior Scientific Officer in Department of Engineering and Technological Studies, University of Kalyani, India. His research interests are in the field of Microwave Antenna, Data Mining, and image processing. He had published several papers in National and International Journals.

Dr. Partha Pratim Sarkar received Ph.D. degree in Electronics Engineering from Jadavpur University, India. He is currently a Senior Scientific Officer in Department of Engineering and Technological Studies, University of Kalyani, India. His research interests are in the field of Microwave Antenna, Wireless and Ad-hoc Networks. He had published several papers in National and International Journals. He is active member of various professional bodies. He has One R&D Project on "Board Band Frequency Selective Surfaces" funded by AICTE.

Dr. Debasree Sarkar received Ph.D. degree in Electronics Engineering from Jadavpur University, India. She is currently a Senior Scientific Officer in Department of Engineering and Technological Studies, University of Kalyani, India. Her research interests are in the field of Wireless and Ad-hoc Networks. She had published several papers in National and International Journals.

Snehasish Banerjee is currently pursuing final year (4th) B.Tech (Computer Science & Engg.) from Academy of Technology, West Bengal University of Technology, India. He is currently working in the field of Steganography and image processing. He has an International conference paper publication title - “Embeding Watermark by Pixel Bit Manipulation”.

Anjan Pal is currently pursuing final year (4th) B.Tech (Computer Science & Engg.) from Academy of Technology, West Bengal University of Technology, India. He is currently working in the field of Visual Cryptography and image processing. He has an International conference paper publication title - “Embeding Watermark by Pixel Bit Manipulation”.