IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735

Variance Based Block Selective Digital Image Watermarking Scheme

Richa Sharma[1], Ajay Khunteta[2]

[1, 2]*(Department of Electronics Engineering, Rajasthan Technical University, India)*

ABSTRACT: *With the increasing use of internet and major development in technology, transmission of digital media is being affected by a large number of illegal interventions. As a valuable solution to this, watermarking provides a secure way for channelizing the digital media (image, audio or video). Digital Watermarking is a method of embedding data (watermark) into a host image without degrading its original quality. This paper presents Digital Image Watermarking in Spatial Domain by finding the Mean and Variance of host image and using the well-known method of Least Significant Bit (LSB) to embed the watermark in a secure position. The experimental results analyze the strength of proposed watermarking algorithm against attacks like Salt and Pepper noise and Gaussian noise.*

Keywords- *Least Significant Bit (LSB), Salt and Pepper Noise, Spatial Domain, Variance, Watermarking*

I. INTRODUCTION

For an impregnable communication, there are mainly three methods available, namely, cryptography, steganography and watermarking. The first one, that is, Cryptography transforms the data in a particular form such that the data becomes unreadable to adversaries, only the authorized parties can access it. The next one, Steganography is the science of concealing information using a carrier signal. On the other hand, Digital Watermarking is a method of embedding data into a multimedia object in such a way that an eavesdropper cannot remove or replace it. Digital watermarks are used to authenticate the identity of its owners. It finds use in medical and military based applications and also used for copyright protection, secret communication and broadcast monitoring. The embedded data i.e. watermark, can be a plain text, an image, audio or a video file.

Digital Watermarking is an effective approach of embedding secret data into a host multimedia file without bringing noticeable artifacts [1]–[3].

A variety of embedding techniques in spatial as well as frequency domain, are used in various applications such as authentication [4], [5], broadcast monitoring, fingerprinting, content-protection, and copy prevention and secret communication.

Celik et al. [6] proposed a watermarking technique in which original cover signal is recovered upon extraction of embedded information. The method used for data-embedding is Least Significant Bit (LSB) modification, and the original signal is recovered by compressing those parts which are vulnerable to embedding distortion. Nasir et al. [7] proposed a technique for inserting the binary image watermark with watermark security. A secret key and Gray code generate sequence numbers through which binary watermark image is permutated, and then embedded four times in distinct positions by a secret key. For the extraction of watermark, the intensities of a block of 8*8 of the watermarked and the original images are compared and then the probability of detecting '0' or '1' is calculated.

Schyndel et al. [9] used an m-sequence generator for producing a watermark. The watermarked image was generated by embedding the watermark to the LSB of the original image in spatial domain. The least significant bits of a suspected image are used to extract the watermark. Bhattacharya et al. [10] proposed a new approach which uses both fragile and robust digital watermarking techniques. The amount of deterioration caused by the transmitted images is determined by the embedded fragile watermark. Delaigle et al. [11] proposed a unique watermarking scheme based on the Human Visual System. Binary m-sequences were produced and then modulated on a random carrier. This image served as the watermark, and then the masked watermark is added to the original image to obtain the watermarked image. Craver et al. [12] noted that a number of watermarking techniques were prone to forgery attacks by adversaries or third party. It is shown that certain methods used for watermarking can be attacked by creating a fake original image. A solution to counterfeit attacks is provided by making the watermark dependent on the original image.

Watermarking is widely used in military and medical applications and also for content authentication [13], copyright protection [15], broadcast monitoring, secure communication and owner identification.

II. BASIC PROCESS OF WATERMARKING

The basic process of Digital Image Watermarking involves three major operations: Embedding, Transmission and Extraction. The embedding phase consists of inserting the watermark into the host signal. An optional encryption mechanism with security key [14] may also be used to add more security to the entire system. At the time of transmission, the adversaries can attack the watermarked image. Therefore, to recover the hidden information from the watermarked image becomes a challenge for the watermark extractor. Fig.1 depicts the basic process of watermarking.

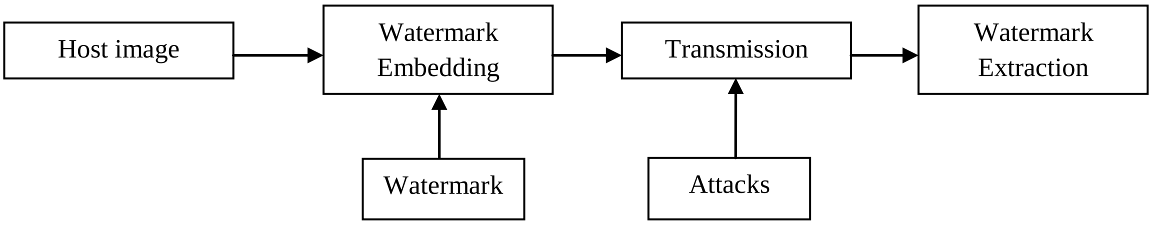


Fig.1 Basic process of watermarking

III. CATEGORIES OF DIGITAL IMAGE WATERMARKING

The digital watermarking techniques can be classified according to the perceptibility of the watermark, capability of the watermark to resist attacks, method of extraction of watermark, the domain of embedded watermark, or according to the capacity of retrieving the host image.

In the case of images, watermarking techniques are commonly differentiated based on two working domains: Spatial domain [18] and Frequency domain. Based on the ability to resist attacks, there are two types of watermark: Robust and Fragile watermark. Meanwhile, based on human perception, digital watermarks are divided into two categories: Visible [19] and Invisible watermark. From application point of view, digital watermarks can be Source and Destination based. Source based is where a unique watermark identifying the owner is introduced to all the copies of a particular content being distributed [20]. Destination based is where each distributed copy gets a unique watermark identifying the particular owner.

IV. THE PROPOSED SCHEME

The proposed scheme embeds watermark in spatial domain. Least Significant Bit (LSB) method is the most common and well known technique of watermarking in the spatial domain. This method uses LSB for embedding and extraction of watermark. The flowchart for the proposed scheme has been shown in Fig.2. The method comprises of following steps:-

Step-I: Insertion of watermark into host image

1) Input the host image of size [M×M] and divide it into ‘m’ equal size blocks.
2) Now, the mean and variance of each block is calculated. The ‘mean’ value is used to find the contribution of individual pixel intensity for the entire image and ‘variance’ is used to find how each pixel varies from the neighboring pixel.
3) Input the watermark of size [N×N] and divide it into ‘n’ equal size blocks.
4) To get the position for watermark embedding, $[\frac{M}{N} \times \frac{M}{N}]$ blocks of host image are chosen which have lowest variances among all so that the watermark can be inserted smoothly at those positions.

5) After this stage, the blocks of watermark are embedded into those positions of host image which were chosen due to lowest variances. This is done by setting the LSB of host image to MSB of watermark using BITSET command.
6) So, now a watermarked image is obtained as output image.

Step-II: Extraction of Watermark

1) In the Extraction phase, the watermark is retrieved by using LSB of watermarked image.
2) By using the MATLAB command BITGET, the watermark is recovered and those blocks can be identified where the watermark was embedded.
3) These blocks of watermark are merged into a single image after extraction.

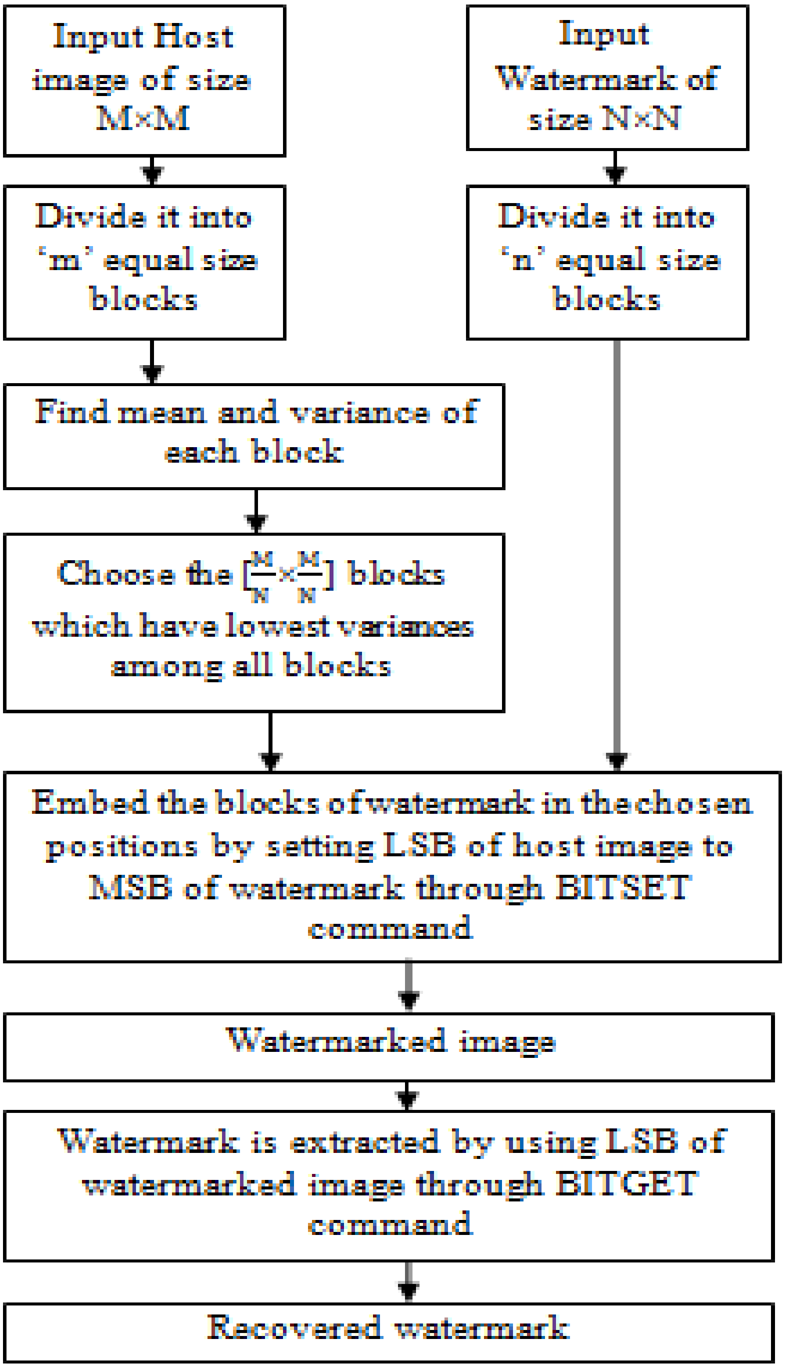

Input Host image of size M×M
Input Watermark of size N×N
Divide it into 'm' equal size blocks
Divide it into 'n' equal size blocks
Find mean and variance of each block
Choose the $[\frac{M}{N}\times\frac{M}{N}]$ blocks which have lowest variances among all blocks
Embed the blocks of watermark in the chosen positions by setting LSB of host image to MSB of watermark through BITSET command
Watermarked image
Watermark is extracted by using LSB of watermarked image through BITGET command
Recovered watermark

Fig.2 Flowchart for the Proposed Scheme

V. EXPERIMENTAL RESULTS

The algorithms of proposed scheme for the embedding and extraction of watermark are implemented using MATLAB 7.5.

A. Test Images

The images used for watermarking process have dimensions:

Size of Host image-512×512

Size of Watermark- 256×256

TIFF images of Cameraman, Lena, Man Tiffany, Woman and Living room are used as host images.

Grayscale TIFF image of Mandrill and Peppers are used as watermark.

Fig.3 shows the test images which are used in the proposed digital image watermarking scheme.

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

Fig.3 Test images [512×512]
(a) Cameraman (b) Lena (c) Man (d) Tiffany (e) Woman (f) Mandrill

B. Performance Evaluation

To evaluate the performance of the proposed scheme, six test images are taken and their Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) values are calculated.

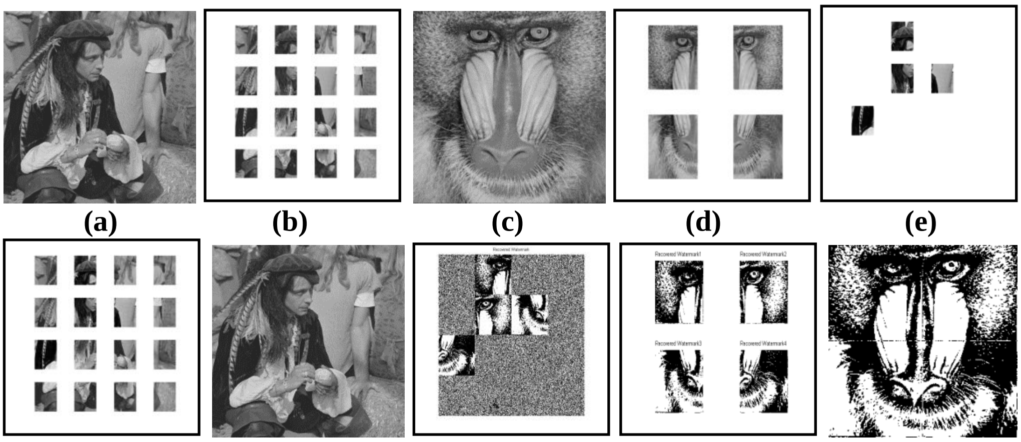
$$\text{MSE}=\frac{1}{M*N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[R(i,j)-R'(i,j)]^{2}$$

Where, i=no. of rows, j=no. of columns, R (i,j) is the host image and R'(i,j) is the watermark

$$\text{PSNR(dB)}=10\log_{10}\frac{\text{maxR}^{2}}{\text{MSE}}$$

where, maxR is the maximum pixel value of the original image.

Fig. 4 shows the test image of Man [512×512] and the watermark image of Mandrill [256×256] which are chosen to show the results of the Proposed Scheme and same process is performed on all the cover images. Results of PSNR and MSE are shown in the Table I.



(a) **(b)** **(c)** **(d)** **(e)**

(f) **(g)** **(h)** **(i)** **(j)**

Fig.4 Results of The Proposed Scheme

(a) Host image, Man [512×512]	(b) Cover image fragmented into blocks
(c) Watermark, Mandrill [256×256]	(d) Watermark divided into blocks
(e) Blocks used for hiding watermark	(f) Watermarked image into blocks
(g) Watermarked Image	(h) Detected watermark in the watermarked image
(i) Recovered Watermark shown into blocks	(j) Extracted watermark

Table I shows the MSE and PSNR values of original and watermarked images.

Table I. Performance analysis for the proposed scheme

Test image	MSE	PSNR
Cameraman	0.12	57.21
Lena	0.12	57.22
Man	0.13	57.23
Tiffany	0.12	57.20
Woman	0.12	57.26
Living room	0.13	57.17

C. Noise Attacks on Watermarked Image

In this paper, firstly, a host image is taken and then Salt and Pepper noise at a gain factor of 0.05 is added and a noisy image is obtained. Same process is applied for the Gaussian noise at a gain factor of 0.07. Table II shows the PSNR (dB) for Salt and Pepper Noise attack at a gain factor of 0.05 and for Gaussian Noise attack at a gain factor of 0.07 between the original image and noisy watermarked image.

Table II Performance Analysis for Noise Attacks

Test image	PSNR analysis for Salt and Pepper noise attack at a gain factor of 0.05	PSNR analysis for Gaussian noise attack at a gain factor of 0.07
Cameraman	44.93	40.07
Lena	44.20	37.59
Man	41.87	35.07
Tiffany	40.37	34.69
Woman	46.11	41.74
Living room	40.67	33.41

Now, the results of the proposed scheme for color test image of Lena [512×512] and the grayscale watermark image of Peppers [256×256] are shown in Fig.5 and same process is performed on all the cover images.

The PSNR and MSE values for the Proposed Scheme is calculated and shown in Table III. PSNR values after addition of Salt and Pepper noise and Gaussian noise are shown in Table IV.

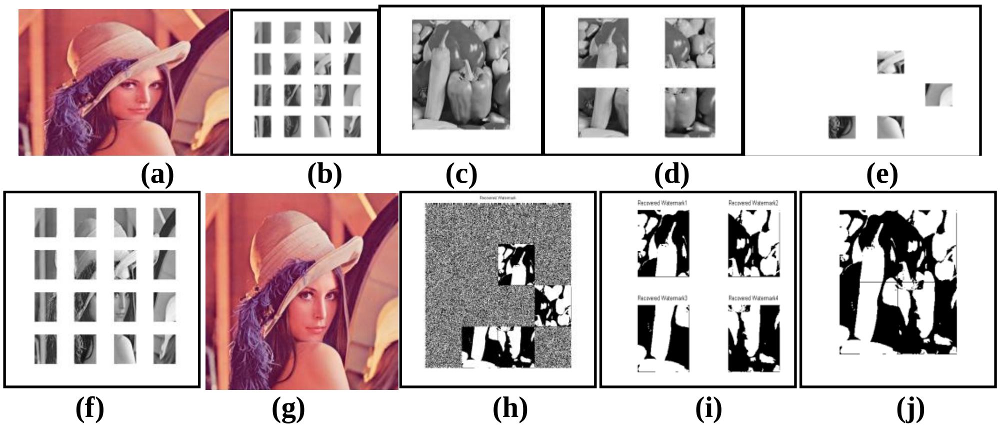


Fig.5 Results of the Proposed Scheme

(a) Host image, Lena [512×512]	(b) Cover image fragmented into blocks
(c) Watermark, Peppers [256×256]	(d) Watermark divided into blocks
(e) Blocks used for hiding watermark	(f) Watermarked image into blocks
(g) Watermarked image	(h) Detected watermark in the watermarked image
(i) Recovered watermark shown into blocks	(j) Extracted watermark

Table III shows the MSE and PSNR values of original and watermarked images.

Table III. Performance Analysis for the Proposed Scheme

Test image	**MSE**	**PSNR**
Cameraman	0.13	57.20
Lena	0.11	57.18
Man	0.13	57.19
Tiffany	0.12	57.19
Woman	0.13	57.17
Living room	0.12	57.23

Table IV shows the PSNR (dB) for Salt and Pepper noise attack at a gain factor of 0.07 and for Gaussian noise attack at a gain factor of 0.08 between the original image and noisy watermarked image.

Table IV. Performance analysis for noise attacks

Test image	**PSNR analysis for Salt and Pepper noise attack at a gain factor of 0.07**	**PSNR analysis for Gaussian noise attack at a gain factor of 0.08**
Cameraman	42.88	40.05
Lena	42.02	36.21
Man	40.18	35.19
Tiffany	38.88	33.12
Woman	43.50	41.23
Living room	38.78	32.47

VI. CONCLUSION

The proposed method used for Digital Image Watermarking yields the PSNR values in range of 50 to 60 dB. The maximum MSE between the cover image and the watermarked image is 0.13. It means that the error between cover image and watermarked image is very small. There is no visible difference between cover image and watermarked image from naked eye. It means that the proposed watermarking scheme is imperceptible. The PSNR values after adding noise are between 32 to 40 dB which shows that the proposed algorithm is robust to attacks like Salt and Pepper noise and Gaussian noise.

REFERENCES

[1] M. D. Swanson, M. Kobayashi, A. H. Tewfik, "Multimedia data embedding and watermarking technologies,"*Proc. IEEE, 86(6),* 1998, 1064–1087.

[2] R. L. Lagendijk, G. C. Langelaar, I. Setyawan, "Watermarking digital image and video data," *IEEE Signal Process. Mag., 17(5),* 2000, 20–46.

[3] F. Hartung, M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE, 87(7),* 1999, 1079–1107.

[4] M. U. Celik, G. Sharma, E. Saber, A. M. Tekalp, "A hierarchical image authentication watermark with improved localization and security," *Proc. IEEE ICIP,* Thessaloniki, Greece, 2001, 502–505.

[5] M. U. Celik, G. Sharma, E. Saber, A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Process.,11(6),* 2002.

[6] M. U. Celik, G. Sharma, E. Saber, A. M. Tekalp, "Lossless Generalized-LSB Data Embedding" *IEEE Transactions On Image Processing, 14(2),* 2005.

[7] I. Nasir, Ying Weng, Jianmin Jiang "A New Robust Watermarking Scheme for Color Image in Spatial Domain", *Signal-Image Technologies and Internet-Based System,* 2007.

[8] I. Cox, J. Kilian, F. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing, 6(12),* 1997, 1673-1687.

[9] R. Schyndel, A. Tirkel, C. Osborne, "A Digital Watermark," *Proc. IEEE Int. Conf. on Image Processing,* ,1994, 86-90.

[10] A. Bhattacharya, S. Palit, N. Chatterjee, G. Roy, "Blind assessment of image quality employing fragile watermarking", *7th International Sym. on Image and Signal Processing and Analysis* (ISPA) Dubrovnik, Croatia, 2011, 431- 436.

[11] J. Delaigle, C. De Vleeschouwer, B. Macq, "Psychovisual Approach to Digital Picture Watermarking", *Journal of Electronic Imaging, 7(3),* 1998, 628-640.

[12] S. Craver, N. Memon, B. Yeo, M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications", *IEEE Journal on Selected Areas in Communications, 16(4),* 1998, 573-586.

[13] F. Alturki, R. Mersereau, "Secure Fragile digital watermarking technique for image authentication", *Proc. of International Conference on Image Processing*, 2001, 1031-1034.

[14] C. D. Coltman, A. G. Bors, "Hierarchical watermarking depending on local constraints", *Proc. of International Conference on Image Processing,* 2001, 1011-1014.

[15] Ki-Hyun Jung, Kyeoung-Ju Ha, Kee-Young Yoo, " Image Data Hiding Method Based on Multi-pixel Differencing and LSB Substitution Methods", *International Conference on Convergence and Hybrid Information Technology*, 2008, 355-358.

[16] H. H. Larijani, G. R. Rad, "A new spatial domain algorithm for gray scale images watermarking", *International Conference on Computer and Communication Engineering*, 2008, 157-161.

[17] K. Thongkor, P. Supasirisun, T. Amornraksa, "Digital Image Watermarking on regularized filter", *14th IAPR International Conference on Machine Vision Applications*, 2015, 493-496.

[18] M. Chandra, S. Pandey, R. Chaudary, "Digital Watermarking Technique for Protecting Digital Images", 3rd *IEEE ICCSIT,* 2010, 226-233.

[19] F. Keissarian, "An Image Watermarking Scheme based on Image Visual Activity for copyright protection", *4th International Conference on Innovations in Information Technology*, 2004, 374-377.

[20] Chih-Wei Tang and Hsueh-Ming Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", *IEEE Trans. on Image Processing*, 51(4), 2003, 950-959.