ISSN:2229-6093

Semi Pixel Difference Method for Digital Image Watermarking With Minimum Degradation in Image Quality

Rajkumar Yadav*
Assistant Professor
U.I.E.T, M.D.U, Rohtak
rajyadav76@rediffmail.com

Gaurav Chawla
M.Tech Student
U.I.E.T, M.D.U, Rohtak
chawla.gaurav17@gmail.com

Ravi Saini
M.Tech Student
U.I.E.T, M.D.U, Rohtak
ravisaini1988@rediffmail.com

Abstract

In this paper, a new method for digital image watermarking is proposed. The proposed method divides the pixel into two parts: semi-pixel 1 and semi-pixel 2. The watermark information bit is inserted at a pixel location according to the difference of two semi –pixels. The pixel for insertion of watermark is selected by using pseudo random number generator that is seeded with a secret key. Experimental results showed that the proposed method has given a good quality watermarked image.

Keywords: *Watermarking, Steganography, Cryptography, Pseudo Random Number Generator.*

1. Introduction

Recent years have witnessed the rapid development of the internet and telecommunication techniques. With this development, information security is become more and more important. Application such as covert communication, copyright protections etc. stimulate the research of information hiding techniques [1]. Information hiding is unlike cryptography. In cryptographic techniques significant information is encrypted so that only the key holder has access to that information. But, once the information is decrypted the security is lost. In information hiding, message is embedded into digital media, which can be distributed and used normally. Information hiding doesn't limit the use of digital data [3]. Information hiding can be classified into two kind of techniques: Steganography and Watermarking. Steganography is the art and science of hiding the data within some cover media like image file, audio file, video file etc. In Greek steganography means" covered writing" [2]. The main purpose of steganography is to hide the fact of communication. The sender embeds a secret message into digital media (e.g. image) where only the receiver can extract that message. The warden of communication channel will notice the transmitted media, but he/she will never perceive the buried secret message inside this media [4.]

Digital watermarking or simply watermarking is defined as a process of embedding information like owner name, company logo etc. in the host data. The process of watermark insertion and extraction is given in Figure 1 and Figure 2 respectively [5]. General image watermarking methods can be divided into two groups according to the domain of application of watermarking. In spatial domain methods [6], the pixel values in the image channel(s) are

Changed. In spectral-transform domain methods, a watermark signal is added to the host image in a transform domain such as the full-frame DCT domain [7]. Watermarking is very similar to steganography in that both seek to hide information in the Cover-object. However steganography is related to secret point-to-point communication between two parties. Thus, steganography techniques are usually having a limited robustness and protect for the embedded information against modifications that may occur during transmission, like format conversion, compression or A/D conversion. On the other hand, watermarking rather than steganography principles is used whenever the media is available to parties who know the existence of the embedded information and may have interest removing it. Thus, watermarking adds additional requirements of robustness. An ideal watermarking system would embed information that could not be removed or altered without making significant perceptual distortion to the media. A popular application of watermarking is to give a proof of correctness of digital data by embedding copyright statements [8].

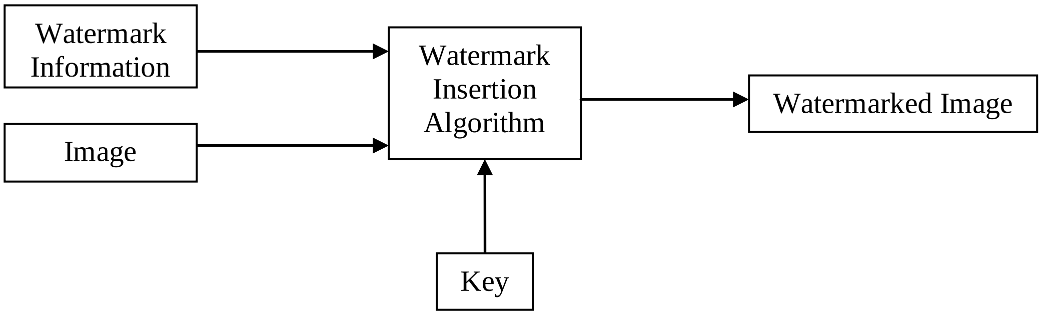

Fig 1: Watermark Insertion

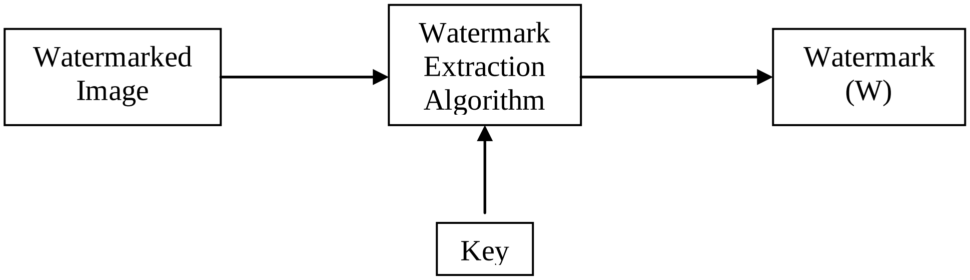

Fig 2: Watermark Extraction Process

In our work, we proposed a new method of digital watermarking in spatial domain. First the pixel is divided into two semi-pixels and their difference is calculated. According to the calculated difference, the watermarked bit is inserted at a pixel value. The pixels for insertion of watermark are selected by using pseudo random number generator which is seeded with a secret key.

The rest of the paper is organized as follows:
Section 2 gives application and properties of watermarking. Section 3 consist our proposed method i.e. Semi-Pixel Difference (SPD) method. Section 4 shows effect of our method on various pixel values. In section 5, experimental results and analysis is shown. At the last of this paper, Section 6 concludes our work and gives some emphasis on future work also.

2. Applications and properties of Digital Watermarking [9]

2.1 Applications

There are many applications of digital watermarking out of which some are given below:

- **Copyright protection**
  Copyright protection is the most important application of watermarking. The objective is to embed information identifies the copyright owner of the digital media, in order to prevent other parties from claiming the copyright. This application requires a high level of robustness to ensure that embedded watermark cannot be removed without causing a significant distortion in digital media. Additional requirements beside the robustness have to be considered. For example, the watermark must be unambiguous and still resolve rightful ownership if other parties embed additional watermarks.
- **Fingerprinting**
  The objective of this application is to convey information about the legal recipient rather than the source of digital media, in order to identify single distributed copies of digital work. It is very similar to the serial number of software product. In this application a different watermark embedded into each distributed copy. In contrast the first application where only a single watermark is embedded into all copies of digital media. As well as copyright protection application of watermarking, fingerprinting requires high robustness.
- **Content Authentication**
  The objective of this application is to detect modification of data. This can be achieved with socalled fragile watermark that have a low robustness to certain modification (e.g. Compression).
- **Copy Protection**
  This application tries to find a mechanism to disallow unauthorized copy of digital media. Copy protection is very difficult in open systems; in closed system, however, it is feasible. In such systems it is possible to use watermarks to indicate the copy status of the digital media (e.g. copy once or never copy). On the other side, copy software or device must be able to detect the watermark and allow or disallow the requested operation according to the copy status of the digital media being copied.
- **Broadcast Monitoring**
  Producers of advertisements or audio and video works want to make sure that their works are broadcasted on the time they purchase from broadcasters. The low-tech method of broadcast monitoring is to have human observers watch the broadcasting channels and record what they see or hear. This method is costly and error prone. The solution is to replace the human monitoring with automated monitoring. One method of automated broadcast monitoring is to use the watermarking techniques. With watermarking we can embed an identification code in the work being broadcasted.

A computer-base monitoring system can detect the embedded watermark, to ensure that they receive all of the airtime they purchase from the broadcasters.

2.2 Properties

Properties of the digital watermarking techniques are given below:

- **Embedding Effectiveness**
  The effectiveness of a watermarking system is the probability that the output of the embedder will be watermarked. The cover work is said to be watermarked when input to a detector result in positive detection. The effectiveness of a watermarking system may be determined analytically or empirically by embedding a watermark in a large number of cover works and detect the watermark. The percentage of cover works that result in positive detection will be the probability of effectiveness.
- **Fidelity**
  In general, the fidelity of a watermark system refers o the perceptual similarity between the original and the watermarked version of the cover work. However, watermarked work may be degraded in the transmission process prior to its being perceived by a person, a different definition of fidelity may be more appropriate. We may define watermarking system fidelity as a perceptual similarity between the unwatermarked and watermarked works at the point at which they are presented to a viewer.
- **Data Payload**
  Data payload refers to the number of bits a watermark embeds in a unit of time or works. For audio, data payload refers to the number of embedded bits per second that are transmitted. Different applications require different data payload. For example, Copy control applications may require a few bits embedded in cover works.
- **Blind or Informed Detector**
  We refer to the detector that requires the original, unwatermarked work as an informed detector. Informed detectors may require information derived from the original work rather than original work itself. Conversely, detectors that do not require the original work are referred to as blind detectors. Informed detector has a good performance in watermark extraction. However, this will result in a huge number of original works have to be stored.

- **False Positive Rate**
  A false positive is the detection of a watermark in a cover work that does not actually contain one. When we talk of a false positive rate, we refer to the number of false positives we expect to occur in a given number of runs of the detector.
- **Robustness**
  Robustness refers to the ability to detect the watermark after common signal processing operations. Audio watermarking needs to be robust to temporal filtering, A/D conversion, time scaling .etc. not all applications of watermarking require all the forms of robustness. This depends on the nature of application of watermarking system.
- **Security**
  The security of a watermark refers to its ability to resist hostile attacks. Hostile attack is the process specifically intended to thwart the watermark’s purpose. The t

pes of attacks can fall in three categories: unauthorized removal, unauthorized embedding, and unauthorized detection.

- **Cost**

  Cost of watermarking system refers to the speed with which embedding and detection must be performed and the number of embedders and detectors that must be deployed. Other issues include the whether the detector and embedder are to be implemented as hardware device or as software application or plug-ins.

3. The Proposed Method

In this section, the proposed is described i.e. SPD (Semi-Pixel Difference) method for hiding watermark information in the spatial domain of the gray scale image. SPD method first divides each pixel into two semi pixels known as semi-pixel 1 and semi-pixel 2 and then watermark information is inserted at the pixel value according to the difference of semi-pixel 1 and semi-pixel 2. If we want to insert watermark bit 0 at a pixel value, then the difference of semi-pixel 1 and semi-pixel 2 must be an even number. Otherwise, we made the semi-pixel difference equal to the even number by adding or subtracting 1 to the pixel value. Similarly, if we want to insert watermark bit 1 at a pixel value, then semi-pixel difference must be an odd number otherwise we made the semi pixel difference equal to odd number by adding or subtracting 1 to the pixel value. The pixels for insertion of watermark information are selected by using Pseudo-Random Number Generator that is seeded with a secret key. The split process of pixel is shown in Figure 3. Table I shows how watermark bits can be inserted according to the Semi-Pixel Difference. Figure 4 shows the watermark insertion process & Figure 5 shows the watermark extraction process.

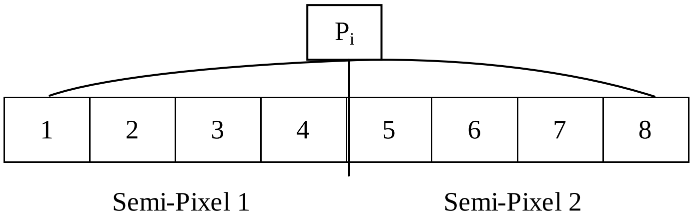

Fig 3: Split Process

Table I: Watermark Insertion according to the Semi-Pixel Difference.

Semi-Pixel Difference	Watermark Bit to be Embedded
0	0
1	1
2	0
3	1
4	0
5	1
6	0
7	1
8	0
9	1
10	0
11	1
12	0
13	1
14	0
15	1

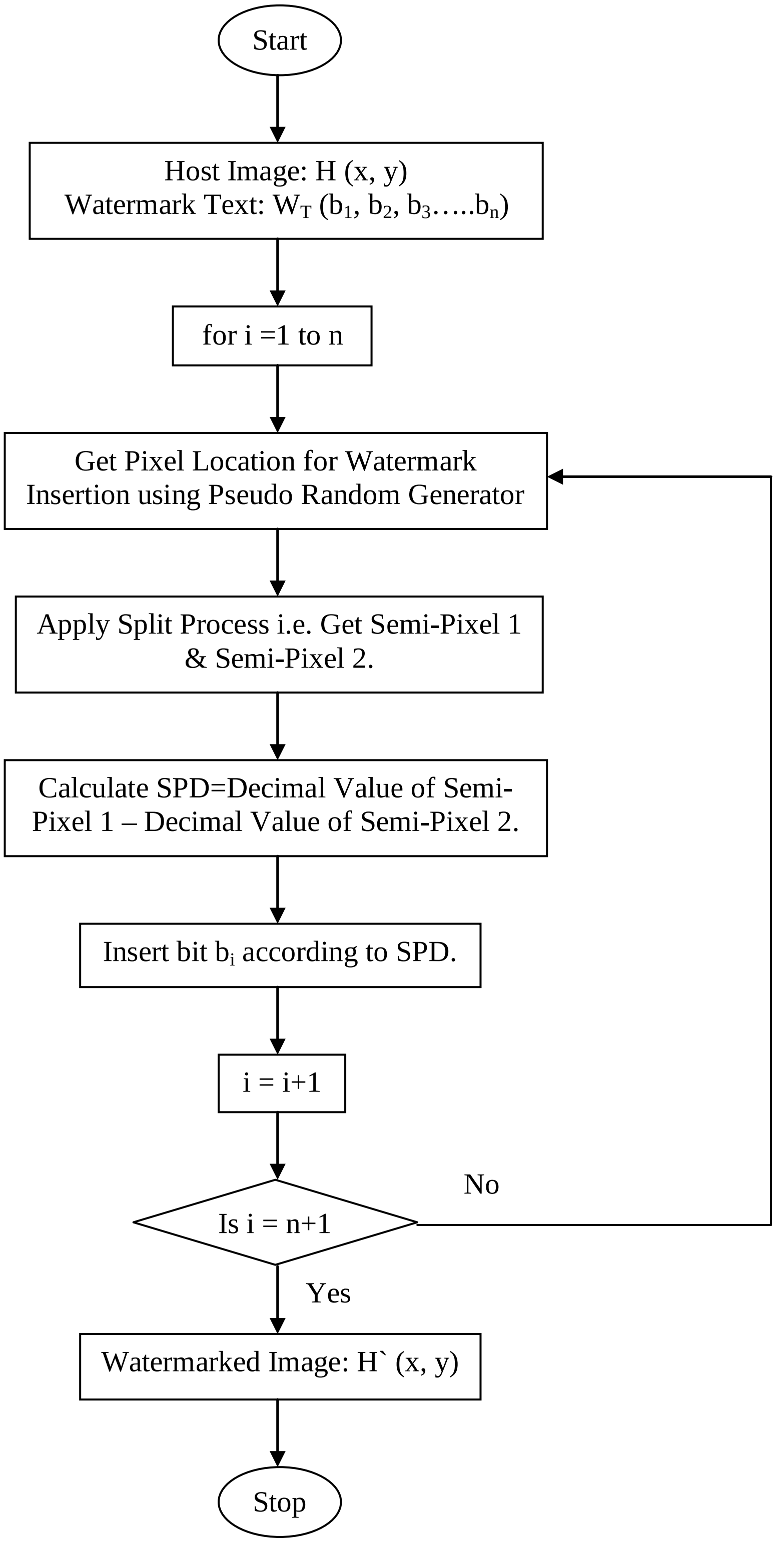
Start
Host Image: H (x, y)
Watermark Text: W_T (b_1, b_2, b_3…..b_n)
for i =1 to n
Get Pixel Location for Watermark Insertion using Pseudo Random Generator
Apply Split Process i.e. Get Semi-Pixel 1 & Semi-Pixel 2.
Calculate SPD=Decimal Value of Semi-Pixel 1 – Decimal Value of Semi-Pixel 2.
Insert bit b_i according to SPD.
i = i+1
No
Is i = n+1
Yes
Watermarked Image: H` (x, y)
Stop

Fig 4: Watermark Insertion Process

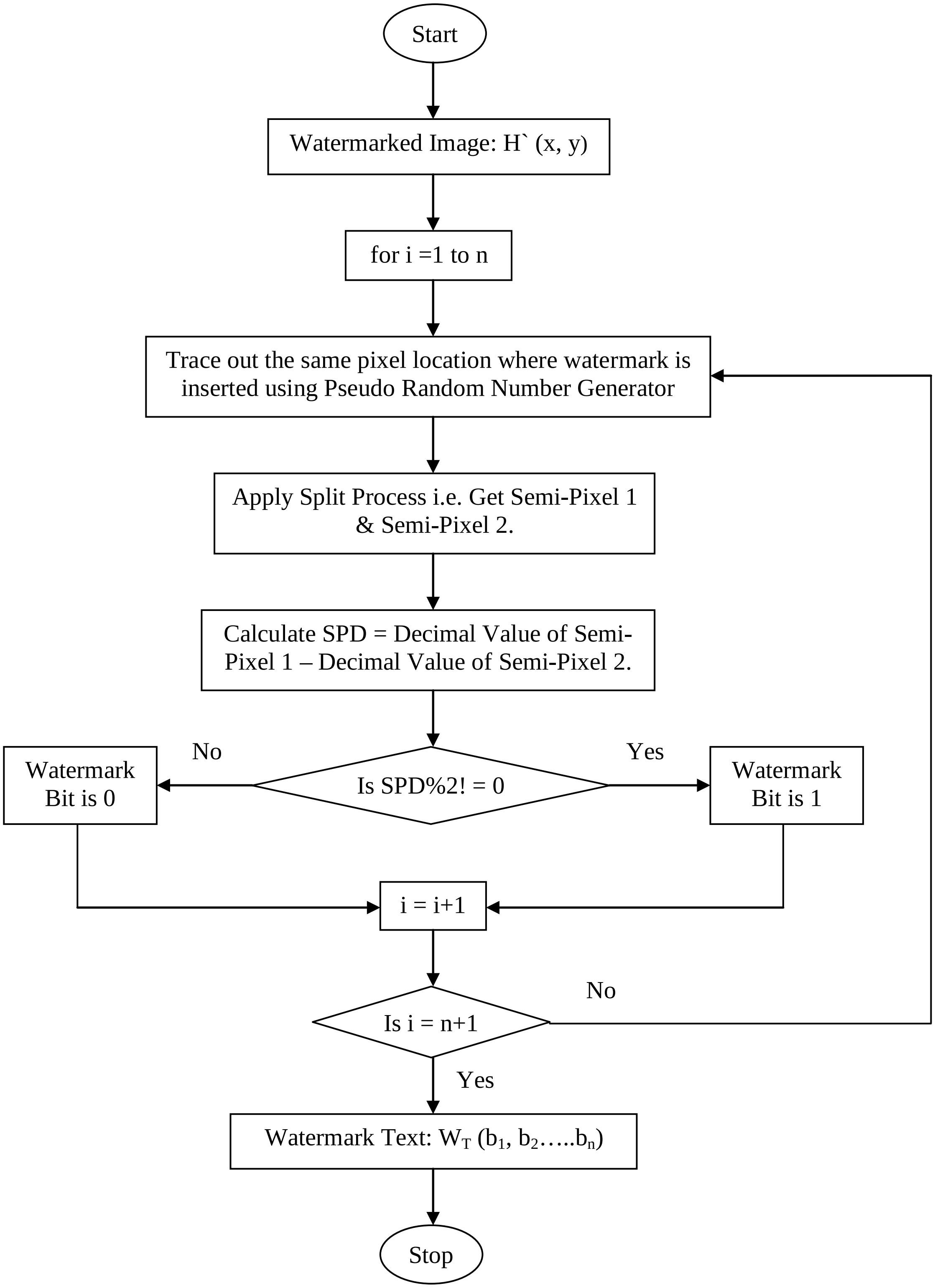
Start
Watermarked Image: H` (x, y)
for i =1 to n
Trace out the same pixel location where watermark is inserted using Pseudo Random Number Generator
Apply Split Process i.e. Get Semi-Pixel 1 & Semi-Pixel 2.
Calculate SPD = Decimal Value of Semi-Pixel 1 – Decimal Value of Semi-Pixel 2.
No
Yes
Watermark Bit is 0
Is SPD%2! = 0
Watermark Bit is 1
i = i+1
No
Is i = n+1
Yes
Watermark Text: W_T (b_1, b_2…..b_n)
Stop

Fig 5: Watermark Extraction Process

3.1 Insertion Algorithm

```
Step 1:  Read the host image: $H(x, y)$
Step 2:  Read the watermark text: $W_T (b_1, b_2,\ldots\ldots b_n)$.
Step 3:  for i=1to n.
Step 4:  Get pixel location $P_i$ for insertion of watermark information using pseudo random number generator.
Step 5:  Apply split process i.e. split the pixel into two equal parts i.e. semi –pixel 1 and semi-pixel 2
Step 6:  Calculate $d_1$ and $d_2$ using equation (1) and (2) respectively.
         $d_1$=DEC (semi-pixel1) ------------ (1)
         $d_2$=DEC (semi-pixel2) ------------- (2)
Step 7:  Calculate SPD using equation (3).
          SPD=Abs ($d_1$-$d_2$) ------------------- (3)
Step 8:  Calculate Decision Variable (DV) using equation (4).
         DV=SPD Mod 2--------------------- (4)
Step 9:  If $b_i$=0 than go to step 10 else go to step 11.
Step10: (a) If DV = = 0, then $b_i$ is present at $P_i$.
         (b) If DV! = 0, then add or subtract 1 to $P_i$ such that DV becomes equal to 0 and insert $b_i$.
Step11: (a) If DV! = 0 then $b_i$ is present at $P_i$.
         (b) If DV = = 0, then add or subtract 1 to $P_i$ such that DV becomes equal to 0 and insert $b_i$.
Step 12: Go to step (3)
Step 13: Watermarked image: H`(x, y).
Step 14: END.
```

3.2 Extraction Algorithm

```
Step 1:  Read the watermarked image: H`(x, y)
Step 2:  for i=1to n.
Step 3:  Trace out the same pixel location $P_i$ using pseudo random number generator where watermark information is present.
Step 4:  Apply split process i.e. split the pixel into two equal part i.e semi –pixel 1 and semi-pixel 2
Step 5:  Calculate $d_1$ and $d_2$ using equation (1) and (2) respectively.
Step 6:  Calculate SPD using equation (3).
Step 7:  Calculate Decision Variable (DV) using equation (4).
Step 8:  If DV = = 0, then 0 is the watermark bit else 1 is the watermark bit.
Step 9:  Go to step (2).
Step 10: Collect the entire watermark bits to get the watermark text: $W_T (b_1, b_2,$ ------$b_n)$.
Step 11: END
```

4. Effect of Watermark Insertion on Various Pixel Values

Now, we see how various pixel values of host image can change during the insertion of the watermark. Table II shows that how various pixel values change during insertion of watermark bit 0. Table III shows that how various pixel values change during insertion of watermark bit 1.

Table – II: Effects of Insertion of Watermark Bit 0 on Various Pixel Values

Original Pixel Value	Semi – Pixel 1	Semi – Pixel 2	SPD	Modified Pixel value after insertion of ‘0’	Modified SPD	Change in Pixel value & comment for insertion of ‘0’
00000000	0000	0000	0	00000000	0	NC, Insert
00000001	0000	0001	1	00000010	2	+1, Insert
00000010	0000	0010	2	00000010	2	NC, Insert
00000011	0000	0011	3	00000010	2	-1, Insert
00000100	0000	0100	4	00000100	4	NC, Insert
00000101	0000	0101	5	00000110	6	+1, Insert
00000110	0000	0110	6	00001000	6	NC, Insert
00000111	0000	0111	7	00000111	8	+1, Insert
00001000	0000	1000	8	00001001	8	NC, Insert
00001001	0000	1001	9	00001011	10	+1, Insert
00001010	0000	1010	10	00001011	10	NC, Insert
00001011	0000	1011	11	00001101	12	+1, Insert
00001100	0000	1100	12	00001101	12	NC, Insert
00001101	0000	1101	13	00001111	14	+1, Insert
00001110	0000	1110	14	00001111	14	NC, Insert
00001111	0000	1111	15	00001110	14	-1, Insert
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
01111111	0111	1111	8	01111110	8	NC, Insert
10000000	1000	0000	8	10000001	8	NC, Insert
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
11111110	1111	1110	1	11111110	0	+1, Insert
11111111	1111	1111	0	11111111	0	NC, Insert

*NC=No Change

Table – III: Effects of Insertion of Watermark Bit 1 on Various Pixel Values

Original Pixel Value	Semi-Pixel 1	Semi-Pixel 2	SPD	Modified Pixel value after insertion of ‘1’	Modified SPD	Change in Pixel value & comment for insertion of ‘1’
00000000	0000	0000	0	00000001	1	+1, Insert
00000001	0000	0001	1	00000001	1	NC, Insert
00000010	0000	0010	2	00000011	3	+1, Insert
00000011	0000	0011	3	00000011	3	NC, Insert
00000100	0000	0100	4	00000101	5	+1, Insert
00000101	0000	0101	5	00000101	5	NC, Insert
00000110	0000	0110	6	00000111	7	+1, Insert
00000111	0000	0111	7	00000111	7	NC, Insert
00001000	0000	1000	8	00001001	9	+1, Insert
00001001	0000	1001	9	00001011	9	NC, Insert
00001010	0000	1010	10	00001011	11	+1, Insert
00001011	0000	1011	11	00001101	11	NC, Insert
00001100	0000	1100	12	00001101	13	+1, Insert
00001101	0000	1101	13	00001111	13	NC, Insert
00001110	0000	1110	14	00001111	15	+1, Insert
00001111	0000	1111	15	00001111	15	NC, Insert
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
01111111	0111	1111	8	01111110	7	+1, Insert
10000000	1000	0000	8	10000001	7	+1, Insert
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
11111110	1111	1110	1	11111110	1	NC, Insert
11111111	1111	1111	0	11111110	1	-1, Insert

5. Results and Analysis

5.1 Subjective Test

We apply subjective test to check the imperceptibility of the watermarked image. Subjective Tests are made by people aging from 18 to 50 who look for visual differences between host image and watermarked image. We took five host images of different sizes and hide the watermark information "My name is Gaurav". The host images & their corresponding watermarked images are presented to 100 analyzers and the results of analyzers are obtained in four numeric values which has the following meanings:

0: No difference at all.
1: Little difference
2: Moderate difference
3: High difference.

After that mean value (M.V.) of 100 decimal values given by 100 analyzers are calculated using equation (5).

$$\boxed{M.V. = \left(\sum_{i=1}^{100} d_i \right) \div 100 ------(5)}$$

Where, d_i is the decimal value given by analyzer i and the result of subjective test is also classified into four levels according to the mean value which is given by Table IV.

Table – IV: Imperceptibility Level according to the Mean Value

Mean Value	Imperceptibility
0<=M.V<1	Highly Imperceptible
1<=M.V<1.5	Moderate
1.5<=M.V<2	Low
2<=M.V<3	Very Low

The result of our subjective test on five different host images is given by Table V.

Table – V: Result of Subjective Test

Image	Image Size (in Pixels)	Watermark Length in Bits	Mean Value
Picture-1	128400	256	0.79
Picture-2	102400	256	0.43
Picture-3	256800	256	0.27
Picture-4	126000	256	0.67
Picture-5	128400	256	0.23

Analyzing the results from Table V, we can conclude that SPD method provides the high imperceptibility i.e. Mean Value lies between 0 and 1. Figures 6 (a), 7 (a), 8 (a) and 9 (a) show the various host images. Figures 6 (b), 7 (b), 8 (b) and 9 (b) show the watermarked image with watermarked information "My name is Gaurav".

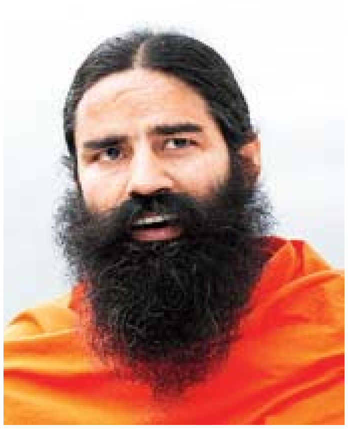

Fig 6(a)

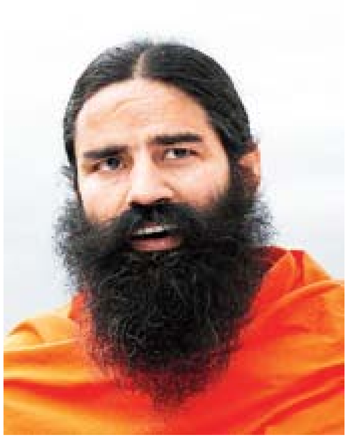

Fig 6(b)

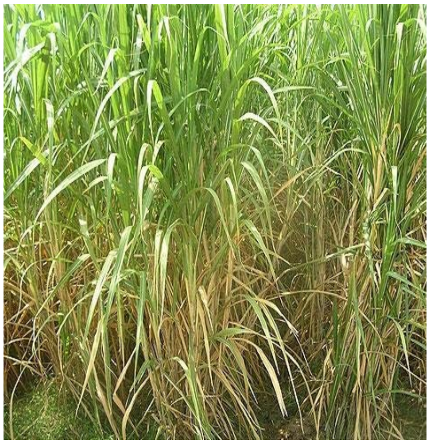

Fig 7(a)

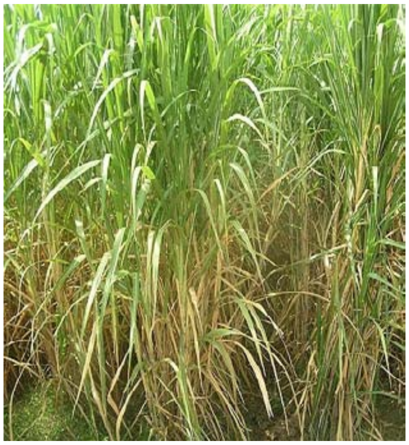

Fig7 (b)

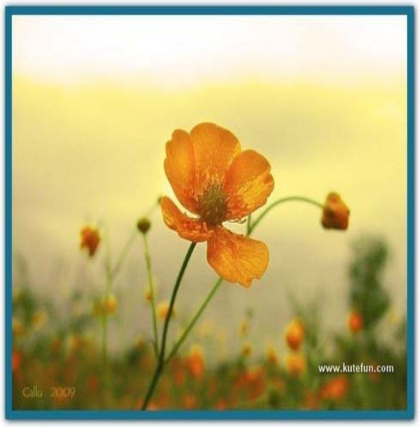

Fig 8(a)

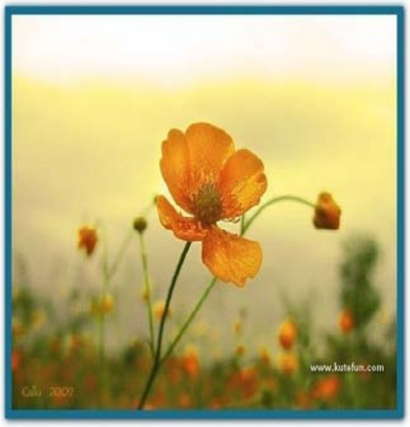

Fig8 (b)

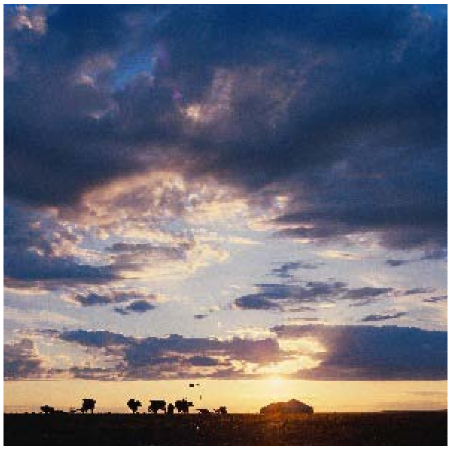

Fig 9(a)

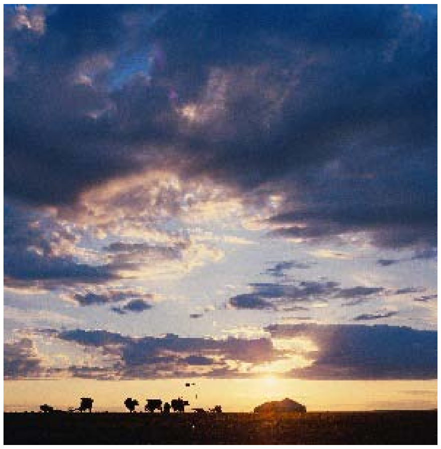

fig 9(b)

5.2 Histogram Analysis

Figures 10 (a), 11 (a), 12 (a) and 13 (a) show the histograms of host images given in figures 6 (a), 7 (a), 8 (a) and 9 (a) respectively. Figures 10 (b), 11 (b), 12 (b) and 13 (b) show histograms of watermarked images given in figures 6 (b), 7 (b), 8 (b) and 9 (b) respectively. By comparing the histograms of host images and watermarked images, we found that there is very less deflection in host images after insertion of watermark. If we increase the size of watermarked information, then deflection in host image also increases but a little bit. A little change in the watermarked image shows that our method provides high level of security.

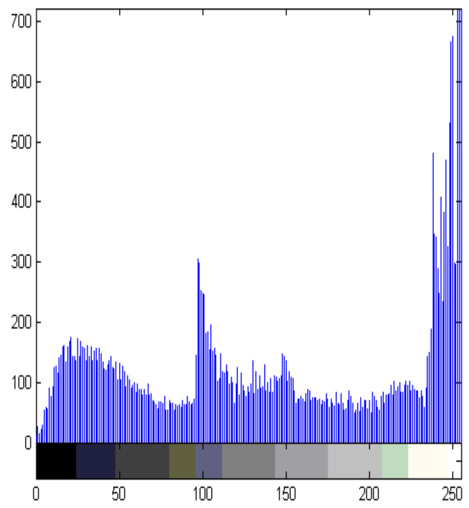

Fig 10(a)

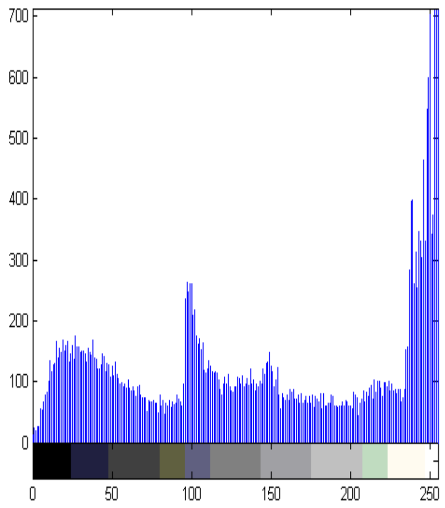

Fig 10(b)

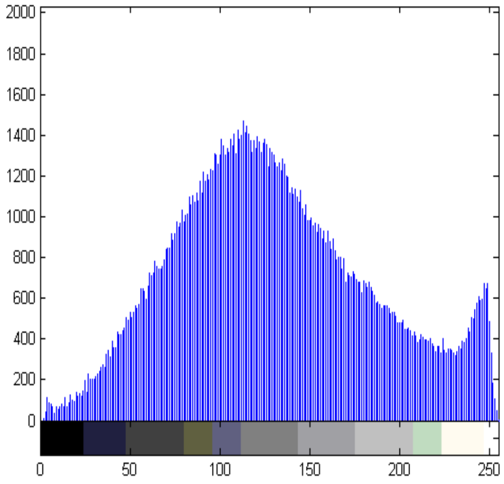

Fig 11(a)

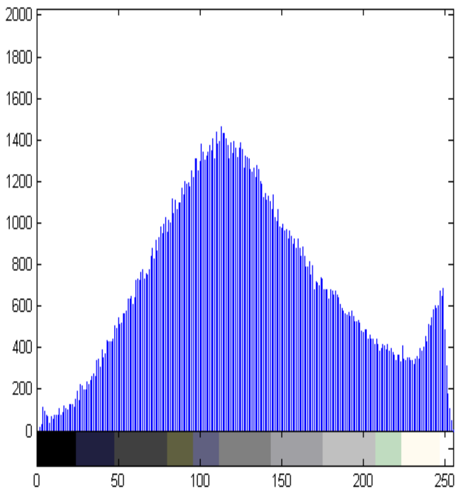

Fig 11(b)

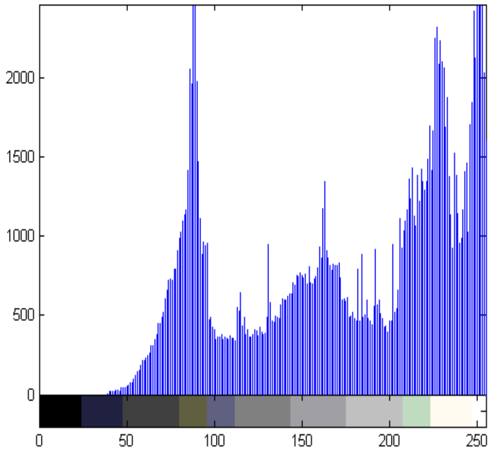

Fig 12(a)

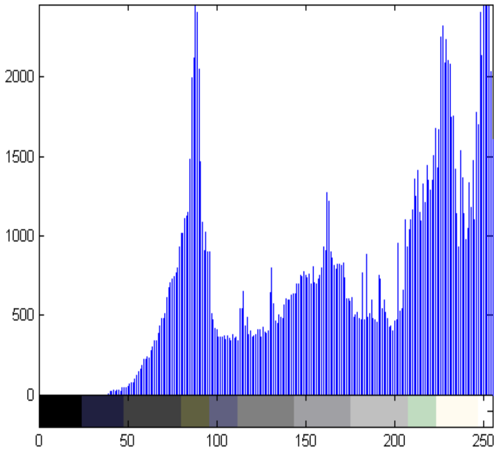

Fig 12(b)

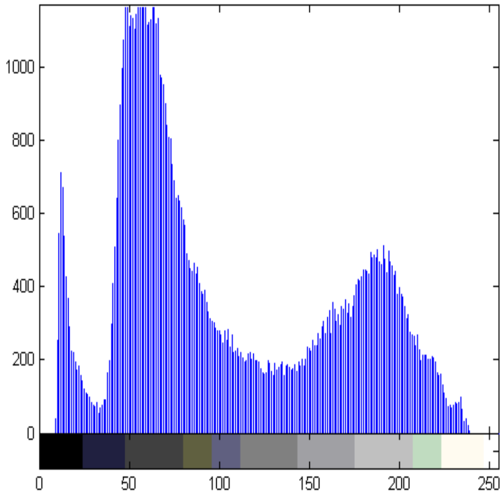

Fig 13(a)

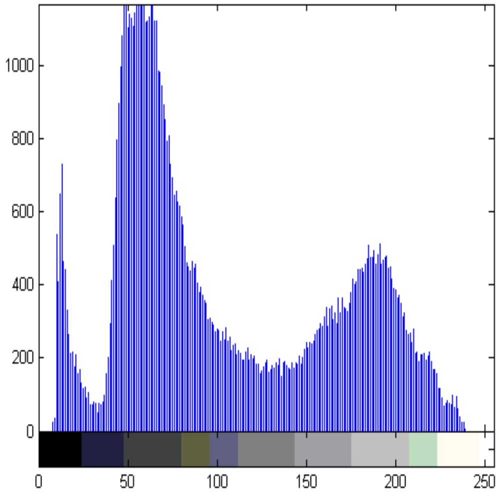

Fig 13(b)

6. Conclusion and Future Scope

We have proposed the Semi-Pixel Difference (SPD) method for digital image watermarking. This method uses the difference of two equal parts of pixel for insertion of watermark information. This method provides us a high level of security. By using this method, the change in the quality of host image is minimum. Future work will concentrate on using this technique in Frequency Domain and increase its robustness.

7. References

1. Souvik Bhattacharya and Gautam Sanyal ,"Adata hiding model with high security features combining finite state machines and PMM method,"in 2010.

2. A. Gutub, M. Faltani, "A Novel Arabic Text Steganography Method Using Letter Points and Extension", WASET International Conference on Computer Information and System Science and Engineering (ICCISSE), Vienna, Austria, May 25-27, 2007

3. Arnold M. 2001, "Audio Watermarking", Dr.Dobb's Journal, Vol. 26, Issue 11, pp. 21-26.

4. Bassia P. and Pitas I. 1998, "Robust Audio Watermarking in the Time Domain". Signal Processing IX, theories and applications: proceeding of Eusipco-98, Ninth European Signal Processing Conf., Greece, pp. 8-11.

5. F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," Proc, IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

6. M. Kutter, F. Jordan, and F. Bossen, "Digital Signature of Color Images Using Amplitude Modulation," Proc. SPIE, vol. 3022, pp. 518-526, 1997.

7. M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT Domain System for Robust Image Watermarking," Signal Processing, vol. 66, no. 3, pp. 357-372, May 1998.
8. Mikdam A. T. Alsalami and Marwan M. AL- Akaidi," Digital Audio Watermarking"

9. Arnold M. 2000, "Audio Watermarking: Features, Applications and Algorithms". Multimedia and Expo. IEEE international Conf., Vol. 2, pp. 1013-1016.

10. Jing Dong and Tieniu Tan, "Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations", National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, P.O. Box 2728, 10190, Beijing, China.

11. M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT Domain System for Robust Image Watermarking," Signal Processing, vol. 66, no. 3, pp. 357-372, May 1998.

12. Stallings.W. Cryptography and network security: Principles and practice. In *Prentice Hall*, 2003.

13. RJ Anderson, FAP Petitcolas, "On the Limits of Stegnography", IEEE Journal on selected Areas in Communications, Vol. 16 No 4, pp 474-481, May 1998.

14. Chandramouli, R., Memon, N.D., 'Steganography capacity: A steganalysis perspective', Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis, 2003.

15. I.Cox,J Kilan, " Secure Spread Spectrum Watermarking for Images,Audio and Video" , in Proc. IEEE International Conference on Image Processing ,1996,vol 3,pp. 243-246.

16. S.Craver ,N. Memon , "Resolving Rightful Ownership with Invisible Watermarking Techniques:Limitations,Attacks and Implications",IEEE Trans.,Vol 16,No. 4,pp. 573-586,1998.

17. Chun-Yu-Chang,"The Application of a Full Counterpropagation Neural Network to Image Watermarking", 2005, IEEE

18. H. Y. Gao, The theory and application of audio information hiding, PH.D. dissertation, Beijing university of Posts and Telecommunications, Beijing, China, 2006.

19. J. F. Delaigle, C. Devleeschouwer, B. Macq et al., "Human visual system features enabling Watermarking J," in Proceedings of IEEE International Conference on Multimedia and Expo, pp. 489–492, Lusanne, Switzerland, 2002.

20. S. Katzenbeisser and F. A. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, ArtechHouse Press, Norwood, Mass, USA, 2000.

21. W. Bender,D. Gruhl,N.Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, no. 3-4, pp. 313–335, 1996.

22. N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," Signal Processing, vol. 66, no. 3, pp. 385–403, 1998.