# Mathematical Formula of Performance of Watermarking System with Repetition of Bits of Watermark

**Himanshu Agarwal**

***Abstract:*** ***The performance of a watermarking system depends on all of its factors, such as watermark embedding strength, size of watermark and repetition of watermark bits. In this paper, a mathematical formula is designed, that governs the relation of performance of watermarking system with amount of the repetition of watermark bits. Performance of the watermarking system is measured by using the extracted watermark bit accuracy rate. The designed formula is verified experimentally. A spatial domain watermarking scheme is used for experimental verification. Further, verification is done for different kind of attacks such as cropping, Gaussian filter, Gaussian noise and salt & pepper noise. Accuracy rate by using the mathematical formula and experimental observations are very near. This supports that the designed mathematical formula is reliable.***

***Keywords: Watermarking, Extracted bit accuracy rate (EBAR), Watermark bit redundancy (WBR), Extracted watermark bit accuracy rate (EWBAR), (PEWBAR: predicted EWBAR), OEWBAR (observed EWBAR)***

## I. INTRODUCTION

Since the past three decades, the digital watermarking has been a key research agenda for the multimedia, pattern recognition, algorithm analysis & development community [1-11]. Digital watermarking offers the solution not limited to security, copyright protection, authentication of digital media [6]. Researchers have worked on development and analysis of different categories of image watermarking schemes. Peak signal to noise ratio (PSNR) [2] and normalized correlation coefficient (NC) [8] are widely used performance measures for watermarking schemes.Researchers have worked on development of image watermarking schemes and their analysis. In most of these work, peak signal to noise ratio (PSNR) [4] is used for quality analysis of watermarked image and, normalized correlation (NC), [11] normalized Hamming similarity (NHS) [11], and symmetric NHS [11] are used for quality analysis of extracted watermark(s).The quality of watermarking scheme depends on watermark embedding strength, size of watermark and repetition of watermark bits in the watermarking scheme.

Further, watermarked data may encounter a chain of intentional or unintentional attacks within the working condition(s). In this paper, analysis is done to study the affect of the repetition of watermark bits on the performance of watermarking system. This analysis is done theoretically and experimentally. Further, analysis is done for different kind of attacks such as cropping, Gaussian filter, Gaussian noise and salt & pepper noise.Normalized Hamming similarity is the most widely used function to analyze a watermarking scheme [4], [8] [11]. Therefore, we use the functions equivalent to normalized Hamming similarity function as a main frame to provide analysis on a watermarking system. Normalized Hamming similarity can be used to estimate the degree of common information in two watermarks. The degree of common information is symmetrical about Normalized Hamming similarity equal to 0.5. We have considered this assertion in the analysis. The rest of this article is organized as follows. In section II, some definitions are given. In section III, we formulate the problem. In section IV, theoretical solutions are given and examples are provided to validate the solutions. Finally, section V concludes the article.

## II. DEFINITION

- Bit embedding capacity (BEC): total number of bits embedded by a watermarking scheme in a given image.
- Watermark length (WL): number of bits in a binary watermark.
- Watermark bit redundancy (WBR): repetition of watermark bits in a watermarking scheme.
- Extracted bit accuracy rate (EBAR):

$$\Gamma_1 = 0.5 + \left| \frac{n_1}{n_2} - 0.5 \right|, \quad (1)$$

where, $n_1$ is the number of correct extracted bits and $n_2$ is the total number of extracted bits.

- Extracted watermark bit accuracy rate (EWBAR):

$$\Gamma_2 = 0.5 + \left| \frac{n_3}{n_4} - 0.5 \right|, \quad (2)$$

where, $x_1$ is an embedded watermark and $x_2$ is a corresponding extracted watermark of the same length, $n_3$ is the number of equal bits in $x_1$ and $x_2$, and $n_4$ is the length of the watermark $x_1$ and . $x_2$ . In (1) and (2), the term 0.5 makes the expressions symmetrical about 0.5. This fact is motivated by [11].

Note that $\Gamma_1 = \Gamma_2$, if the total number of extracted bits is equal to the length of the watermarks.

## III. PROBLEM FORMULATION

We use following model of computation.

**Revised Manuscript Received on August 05, 2019**

**Himanshu Agarwal** Department of Mathematics Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India.

- ***M1***. $M_m$ ($m$ is a variable) is a watermarking scheme that has an embedding capacity of $C_m$, EBAR of $P_m$ and EWBAR of $P'_m$. Note that $C_m$, $P_m$ and $P'_m$ are not fixed for fixed $M_m$.
- ***M2***. Let **W** be a watermarking system that is intended for owner identification, ownership authentication or tracking under the working condition $T_w$. Let **W** consist of a set of watermarks $S_w$, a watermarking scheme $M_w$, and a set of host data $A_w = \{a_i : i = 1; 2; \cdots n_a\}$ that has $n_a$ host data. Let $N_w$ be watermark bit redundancy, and $C_w = C_w(M_w; S_w; A_w)$, $P_w = P_w(M_w; T_w; S_w; A_w)$, and $P'_w = P'_w(M_w; N_w; T_w; S_w; A_w)$ be the embedding capacity, minimum EBAR and minimum EWBAR respective of the $M_w$.

The formulated problem is as follows:

- Find relation between $N_w$, $Pw$ and $P'_w$ subjected to $S_w = S_g$, $M_w = M_g$, $Tw = T_g$, $A_w = A_g$.

We make the following assumptions.

- A1. Each extracted bit obeys the binomial probability model i.e. the probability of each extracted bit being correct is fixed.
- A2. If watermark bit redundancy is greater than 1, then bits of the extracted watermark are estimated from extracted bits using the voting method.

## IV. SOLUTION

- Watermarking scheme $M_w$ is $M_1$ that corresponds to [9] with a slight modification. The modification is that the watermark is put into the third least significant bit (LSB) plane of the host image instead of the LSB plane. The block diagram of the watermarking algorithm is shown in figure 1.
- The set of host data $A_w$ is $A_1$ that consists of a host image as 'cameraman' [12]. The host image is an 8-bit gray scale image of size 256 x 256 pixels.
- The watermark is a binary logo HBP as shown in figure 2. The size of the watermark is 32×32 pixels.

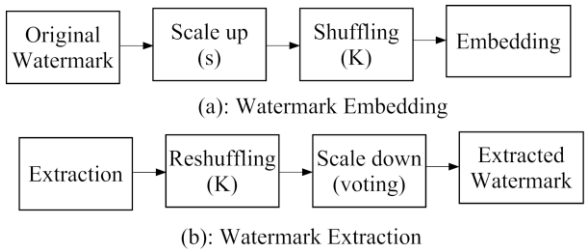
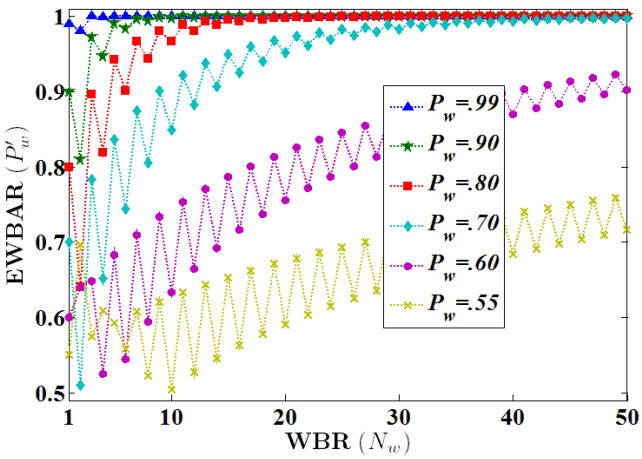
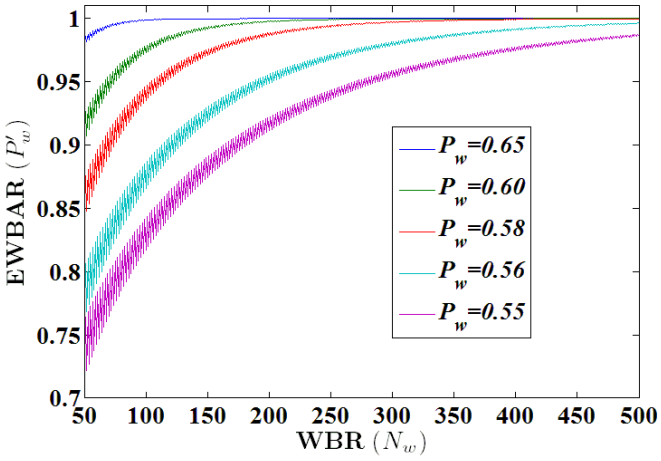



**Figure 1: A modified watermark embedder and watermark extractor. s: scale up factor, K: shuffling key.**

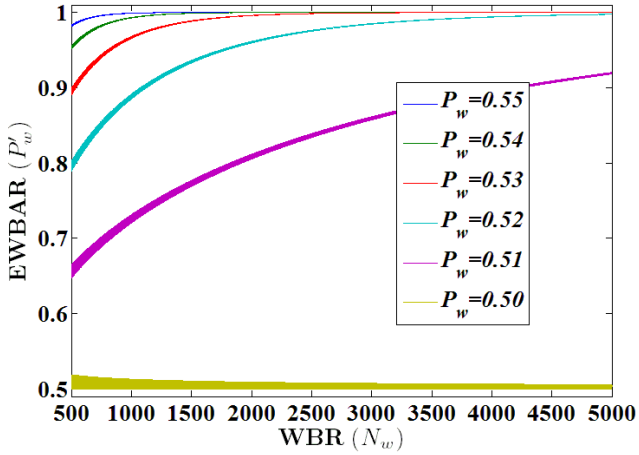
**Figure 2: Watermark**




**(a)**




**(b)**




**(c)**

**Figure 3: Watermark bit redundancy ($N_w$) vs EWBAR ($P'_w$) for various EBAR ($P_w$).**

Under the assumptions A1 and A2, the following relation holds between EWBAR of $P'_w (= P'_w(M_g; N_w; T_g; S_g; A_g))$ and WBR of $N_w$

$$P_w' = 0.5 + \left| \sum_{i=q}^{N_w} \binom{N_w}{i} P_w^i (1 - P_w)^{N_w - i} - 0.5 \right| \quad (3)$$

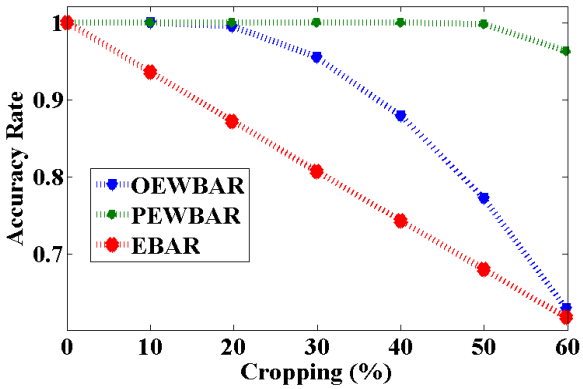
where,

$$q = \begin{cases} \frac{N_w + 1}{2}, & \text{if } N_w \text{ is odd} \\ \frac{N_w}{2} + 1, & \text{if } N_w \text{ is even} \end{cases} \quad (4)$$

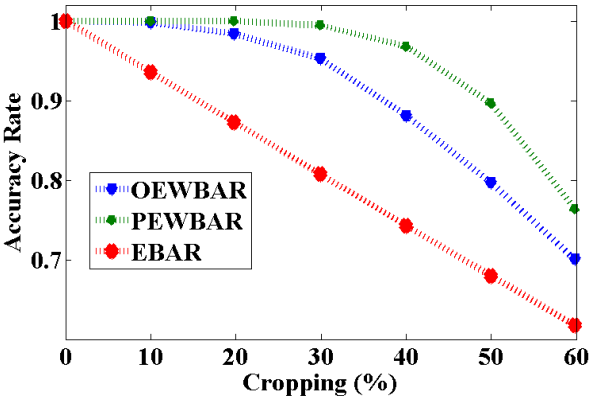
$P_w = P_w(M_g; T_g; S_g; A_g)$. The term 0.5 in eq. (3) makes $P'_w$ symmetrical about 0.5. If $P_w \neq 0{:}5$, then $P'_w$ increases as $N_w$ increases. However, increasing $N_w$ reduces the length of the watermark. The $h_w$ (length of the watermark), $C_w$ (bit embedding capacity) and $N_w$ satisfy the following:

$$h_w \leq \frac{C_w}{N_w} \quad (5)$$

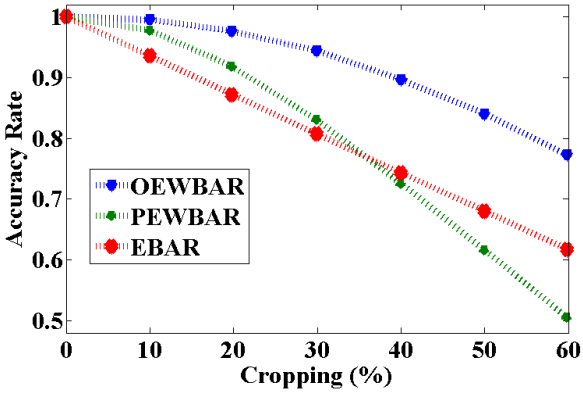
Figure 3 shows graphs of $N_w$ vs. $P'_w$ for various $P_w$. For large $N_w$, the term $\left| \sum_{i=q}^{N_w} \binom{N_w}{i} P_w^i (1-P_w)^{N_w - i} - 0.5 \right|$ can be approximated by the Gaussian error function.




**(a)**: $h_w$=32×32, $N_w$=64

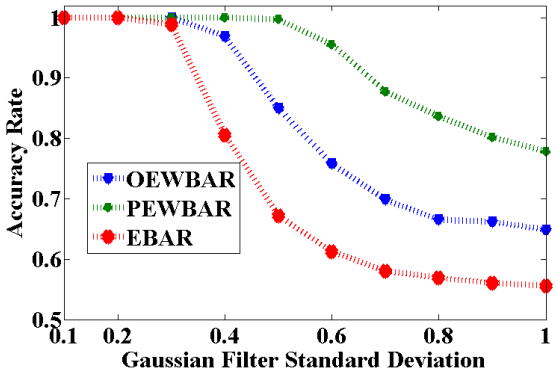



**(b)**: $h_w$=64×64, $N_w$=16

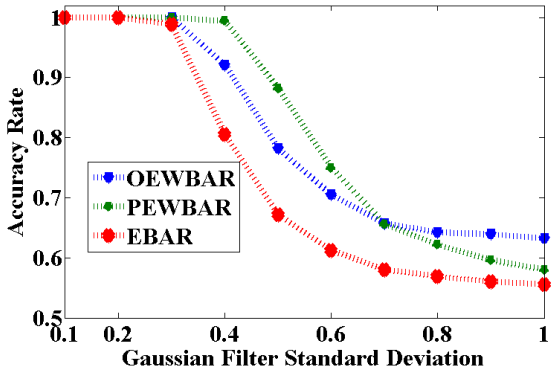



(c): *hw*=128×128, *Nw*=4

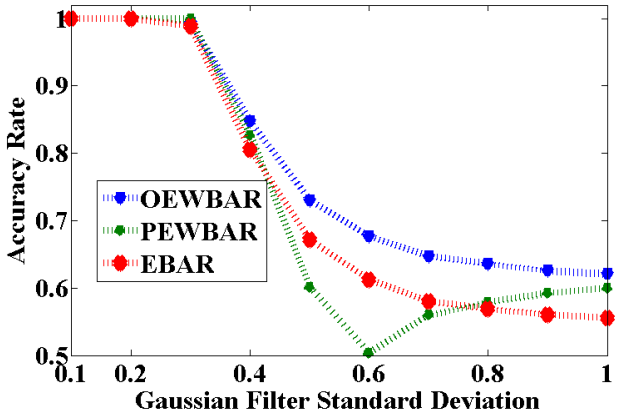
**Figure 4**: Comparison between OEWBAR and EEWBAR for the cropping from center (Cw = 256 × 256)




**(a)**: $h_w$=32×32, $N_w$ =64

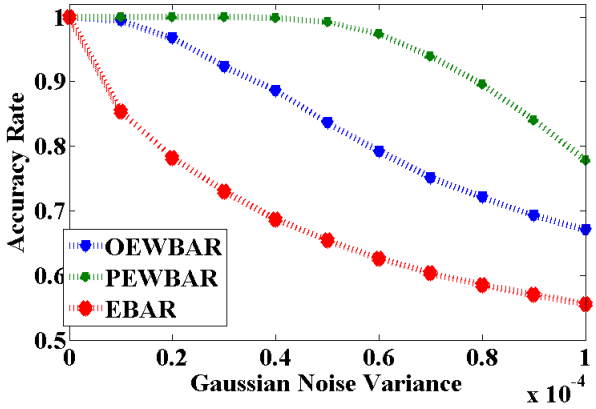



**(b)**: $h_w$ =64×64, $N_w$ =16

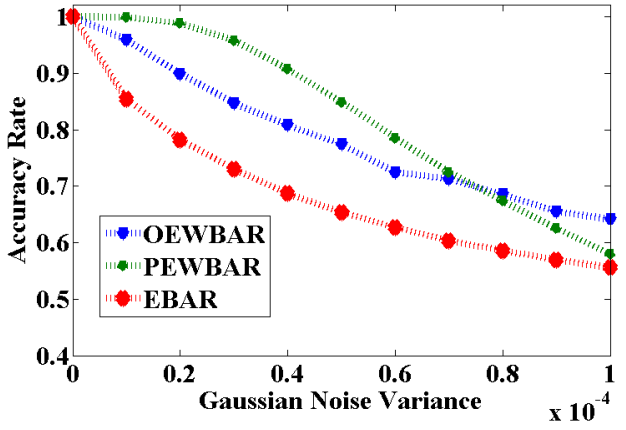



**(c)**: $h_w$ =128×128, $N_w$ =4

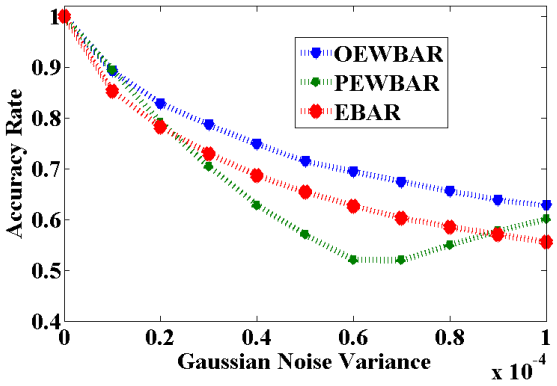
**Figure 5: Comparison between OEWBAR and EEWBAR for the Gaussian filtering (*Cw* = 256 × 256).**




**(a)**: $h_w$ =32×32, $N_w$ =64

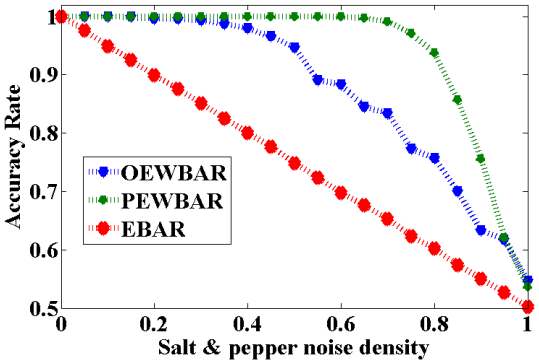



**(b)**: $h_w$ =64×64, $N_w$ =16

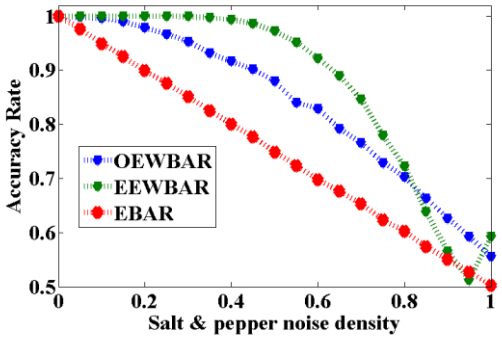



**(c)**: $h_w$ =128×128, $N_w$ =4

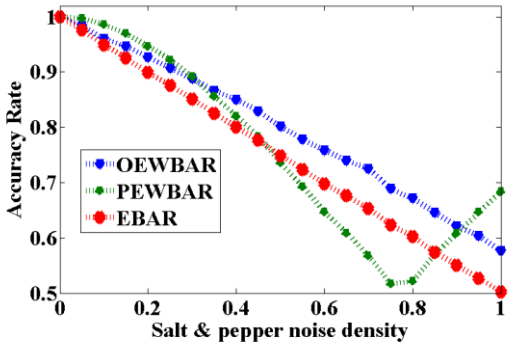
**Figure 6: Comparison between OEWBAR and EEWBAR for the Gaussian noise (*Cw* = 256 × 256).**




**(a)**: $h_w$ =32×32, $N_w$ =64




**(b)**: $h_w$ =64×64, $N_w$ =16




**(c)**: $h_w$ =128×128, $N_w$ =4

**Figure 7: Comparison between OEWBAR and EEWBAR for the salt & pepper noise (*Cw* = 256 × 256)**

To verify (3), a set of experiments is done using the watermarking scheme $M_1$, a host image and various resized versions of a binary logo watermark. The host image is shown in figure. 2. The bit embedding capacity $C_w$ of the watermarking scheme is 256 × 256. The watermarks are different scale up versions of the HBP logo that has a length of 32 × 32. The lengths of the watermarks are 256 × 256, 128 × 128, 64 × 64 and 32 × 32, and corresponding watermark bit redundancies are 1 (no redundancy), 4, 16 and 64 respectively. Before embedding, each watermark is preprocessed according to figure 1 (a). This is done to achieve the binomial probability model assumption for the maximum possible image processing attacks. In the extraction stage, post-processing is done according to Fig. 1 (b) to extract a watermark. Figures 4-7 show the comparison of (3) (PEWBAR: predicted EWBAR) with the OEWBAR (observed EWBAR) for cropping from the center, the Gaussian filter, the Gaussian noise and the salt & pepper noise attacks, respectively, on the watermarked images for different $h_w$ and $N_w$. In cropping from the center, a certain percentage of pixels from the center of a watermarked image is blackened. From figures 4-7, it is observed that OEWBAR strictly matches the PEWBAR up to a certain level of image processing attacks. Moreover, PEWBAR and OEWBAR confirm that EWBAR increases on increasing watermark bit redundancy. One interesting observation is that at $N_w$ = 16, the OEWBAR and PEWBAR are very close.

## V. CONCLUSIONS

The effect of increasing the watermark bit redundancy on EWBAR is predicted based on a binomial probability model. Both PEWBAR and OEWBAR confirm that on increasing watermark bit redundancy, EWBAR increases. Experimental results validate that PEWBAR is close to OEWBAR.

## ACKNOWLEDGMENT

The author acknowledges research support of the Jaypee Institute of Information Technology of India.

## REFERENCES

1. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography", 2nd ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2007.
2. C.-T. Hsu and J.-L. Wu, "Multiresolution watermarking for digital images," IEEE Transactions on Circuits and Systems-II Analog and Digital Signal Processing, vol. 45, no. 8, pp. 1097–1101, August 1998.
3. M.-C. Hua, D.-C. Loub, and M.-C. Changb, "Dual-wrapped digital watermarking scheme for image copyright protection," Elsevier Computers & Security, vol. 26, no. 4, pp. 319–330, June 2007.
4. D. Kundur and D. Hatzinakos, "Digiatl watermarking for telltale tamper proofing and authentication," Proceddings of IEEE, vol. 87, no. 7, pp. 1167–1179, July 1999.
5. D. Kundur and D. Hatzinakos, "Toward robust logo watermarking using multiresolution image fusion principles," IEEE Transactions on Multimedia, vol. 6, no. 1, pp. 185–198, February 2004.
6. H. Lu, R. Shen, and F. L. Chung, "Fragile watermarking scheme for image authentication," Electronics Letters, vol. 39, no. 13, pp. 898–900, June 2003.
7. W. Lua, H. Lua, and F.-L. Chungb, "Robust digital image watermarking based on subsampling," Elsevier Applied Mathematics and Computation, vol. 181, no. 2, pp. 886–893, October 2006.
8. S. Rawat and B. Raman, "A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion," Elsevier AEU - International Journal of Electronics and Communications, vol. 66, no. 11, pp. 955–962, November 2012.
9. P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1593–1601, October 2001.
10. X. Wua and Z.-H. Guana, "A novel digital watermark algorithm based on chaotic maps," Elsevier Physics Letters A, vol. 365, no. 5-6, pp. 403–406, June 2007.
11. H. Agarwal, B. Raman, P. K. and M. Kankanhalli, "Analysis of comparators for binary watermarks, Proceedings of International Conference on Computer Vision and Image Processing Springer, pp. 399-410, 2017.
12. www.imageprocessingplace.com/root files v3/image databases.htm, last accessed on 28th July 2019.

## AUTHORS PROFILE

**Himanshu Agarwal** is an Assistant Professor in the Department of Mathematics, Jaypee Institute of Technology, Noida, India. He has received Ph.D. degree from the Department of Mathematics, Indian Institute of Technology Roorkee in 2015. He was a visiting research student in the Applied Computer Science Department, The University of Winnipeg, Canada in 2012-2013 for six months. He has received M.Sc. degree in Industrial Mathematics & Informatics from Indian Institute of Technology Roorkee in 2009. So far he has published twelve research papers in reputed International Journals and International conferences. His area of research includes image processing, computer vision, information visualization, information security and statistical learning.