Semi-Fragile Watermarking with Tamper Localization and Recovery using AMBTC Method

Shaik Hedayath Basha, Vinodh Kumar R, Teekaaram V, Vishnu N, Kamalesh R

Abstract: *The watermarking scheme in digital media communication has become an essential tool in helping content creators prove ownership if any dispute arises in copyright infringement. In this paper, Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) is performed in the watermarking process which improves the authentication of the image and the detection of the tampered region. The semi-fragile watermarking scheme provides robustness to the watermark during extraction process even after the unintentional compression attacks like JPEG compression. The watermark payload is significantly lowered in order to increase the quality of the image. The recovery is done using the absolute moment block truncation coding (AMBTC) of the image in the untampered region. Thus, both the mean and first absolute moment are used in recovering the tampered regions in the watermarked image.*

Keywords: Watermarking, Discrete Wavelet Transformation, Singular Value Decomposition (SVD), Tampering, AMBTC, Peak signal-to-noise ratio (PSNR).

I. INTRODUCTION

Data protection in the digital world is a necessity to protect our private contents from being misused by malicious attackers. Several techniques are employed for securing the private data. The common methods to secure our information are cryptography, steganography and watermarking. Steganography is the method of converting the secret message into a fake message without altering the structure of the data. While in cryptography, the entire message is encrypted at the transmission side and decrypted at the receiver side. Watermarking involves hiding a secret message like text, audio or image in the data to preserve the

Shaik Hedayath Basha*, Electronics and Communication Department, R.M.K. College of Engineering and Technology, Chennai, India, Email: shaikhedayathbasha@rmkcet.ac.in

Vinodh Kumar R, Electronics and Communication department, R.M.K. College of Engineering and Technology, Chennai, India, Email: vinod16ec152@rmkcet.ac.in

Teekaaram V, Electronics and Communication department, R.M.K. College of Engineering and Technology, Chennai, India, Email: teeka16ec145@rmkcet.ac.in

Vishnu N, Electronics and Communication department, R.M.K. College of Engineering and Technology, Chennai, India,

Kamalesh R, Electronics and Communication department, R.M.K. College of Engineering and Technology, Chennai, India,

authentication of the ownership. The digital watermarking technology is a frontier research field, and it serves an important role in information security. The digital watermarks are embedded either visible or invisible in the information. These watermarks are classified into three different categories: robust, fragile and semi-fragile watermark. A robust watermark should be able to resist intentional or unintentional manipulations, while a fragile watermark is intended to be destroyed even after the smallest unintentional manipulation [7]. Robust watermarking can be used to validate copyrights and intellectual property rights. The semi-fragile watermarking uses watermarks that can resist unintentional manipulations caused by common image processing operations like JPEG compression and are fragile against intentional and malicious manipulations. For a strong watermark embedding, a good watermarking technique is needed to be applied. In this paper, a semi-fragile watermarking technique in wavelet domain is proposed to embed the watermark in the image and the watermark is robust to the unintentional tampering such as JPEG compression attacks. The recovery was done using the AMBTC method of untampered regions in the image.

II. LITERATURE SURVEY

This section provides a brief of various works proposed by various researchers in the recent years. The watermark embedding techniques are classified into two divisions based on the domain of processing the pixels [23]. In Spatial domain watermarking, the processing is done on the pixel values and it loads the raw data into the original image [20]. This type of watermarking can be done in a single-color band. The techniques that are used in the spatial domain watermarking are Least significant bit (LSB) insertion, SSM modulation- based technique, texture mapping coding technique, patchwork algorithm and correlation- based technique. Whereas the frequency domain watermarking is based on the rate of change of the pixel values. The main reason for using a frequency domain is that the human visual system has a better view when captured in the spectral domain. Most of the commonly used transformations techniques in the frequency domain watermarking are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT). Compared to the spatial domain techniques frequency domain techniques are used widely because of their performance in various attacks. An approach was proposed where the host image is transformed using a wavelet domain and flags are created using a secret key. After the extraction of the watermark image, the original flags were compared

Retrieval Number: E9263069520/2020©BEIESP
DOI: 10.35940/ijeat.E9263.069520
Journal Website: www.ijeat.org

54

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication
© Copyright: All rights reserved.

with the extracted flags obtained from the attacked image.

This method was robust against various attacks as watermark was embedded in the middle frequency area of the wavelet domain. This resulted in the less degradation of watermarked image [3].

The semi-fragile watermarking scheme in the DWT domain was able to detect and precisely locate intentional tampering in watermarked images [16]. Embedding in multiple regions has made the approach robust and helped to perform well in even severe cases of tampering [22]. Various watermarks such as authentication watermarks and recovery watermarks for tamper area localization and content recovery can be embedded [19]. But the quality parameters such as robustness, imperceptibility and embedding strength of the watermarking information should be balanced to achieve a good image quality [15].Thus, the robustness of the watermark was improved by the combined multiple techniques of multi-level Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) [8] [24].

The cumulation of these techniques improved the robustness of the watermarks and the quality of the watermarked image. This algorithm is reported to save the execution time during embedding of the watermark [1]. In this paper [10], the author proposed a method based on dividing the image into non overlapping blocks using a two-level quantization technique. Image compression using AMBTC provided better image quality than the BTC technique. In this paper [11], the author proved high quality restoration of the tampered image with the AMBTC technique by maintaining the features of the host cover image.

III. METHODOLOGY

A. DISCRETE WAVELET TRANSFORM

The Discrete Wavelet Transform technique is a discrete algorithm used to make the wavelet computations with simplicity. The wavelet transform is a multi-resolution decomposition for 1D and 2D signals. In wavelet transformation of the 1D signals, 1D filter is applied in each dimension. For 2D signals, the image is decomposed in terms of wavelet functions. The input signals such as images with single level decomposition divides the images into 4 non-overlapping sub-bands such as LL (Approximation sub-band), LH (vertical sub-band), HL (horizontal sub-band), HH (diagonal sub-band) as shown in Figure 1. Here, the midrange frequencies (LH or HL) of the decomposed image is selected for watermarking as they can withstand the common attacks such as cropping, rotation and salt and pepper attacks.

The Haar wavelet is a simple wavelet with zero mean and normalization. It is not continuous and thus can be used in the analysis of the signals with sudden transitions.

$$\Psi_{haar}(t) = \begin{cases} 1, & for\ 0 < t < 0.5 \\ -1, & for\ 0.5 < t < -1 \\ 0, & otherwise \end{cases} \quad (1)$$

The scaling function $\Phi(t)$ of the Haar wavelet is defined as follows in Equation (2).

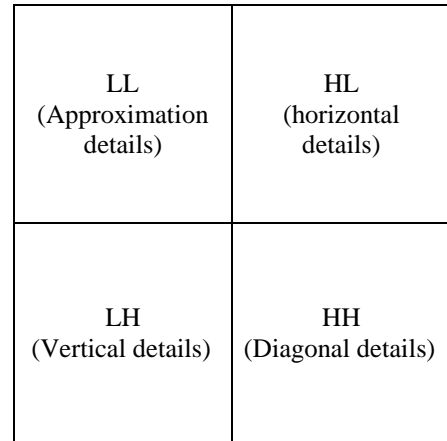$$\Phi(t) = \begin{cases} 1, & 0 \le t < 1 \\ 0, & otherwise \end{cases} \quad (2)$$

LL (Approximation details)	HL (horizontal details)
LH (Vertical details)	HH (Diagonal details)

Figure 1. First level DWT decomposition of the image

B. SINGULAR VALUE DECOMPOSITION

The Singular value decomposition is a mathematical method for decomposing a matrix into three matrices such as 2 orthogonal matrices and a diagonal matrix. If I is an image of size N × N, then the SVD of the image I is given by

$$I = USV^T \quad (3)$$

$$= [u_1, u_2, ..., u_N] \begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix} [v_1, v_2, ..., v_N] \quad (4)$$

$$= \begin{pmatrix} u_{11} & \cdots & u_{1N} \\ \vdots & \ddots & \vdots \\ u_{N1} & \cdots & u_{NN} \end{pmatrix} \begin{pmatrix} s_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & s_N \end{pmatrix} \begin{pmatrix} v_{11} & \cdots & v_{1N} \\ \vdots & \ddots & \vdots \\ v_{N1} & \cdots & v_{NN} \end{pmatrix}$$

where U and V are the N x N orthogonal matrices representing the horizontal and the vertical details of the image, respectively. The unitary matrices $[u_1, u_2, ..., u_N]$ and $[v_1, v_2, ..., v_N]$ from Equation (4) represent the column vectors. The matrix S represents the diagonal matrix with values $S_i (1 \le i \le N)$ and $S_1 \ge S_2 \ge S_3 \ge ... \ge S_n$ are the singular values of the image. The SVD transform is used in image processing due to its algebraic properties. Also, the luminance of the image is contained in the S and V matrix and the small alterations to the image does not affect the SV matrix due to its very good stability. Another advantage of the SVD transformation is that it can be applied even if the input image is a rectangular matrix.

C. ABSOLUTE MOMENT BLOCK TRUNCATION CODING (AMBTC)

The AMBTC method was proposed by Lema and Mitchell in 1984 which improved the compression of the digital images. The AMBTC involves the computation of mean and first absolute moment for every $m \times n$ block in the image I of size $M \times N$. The mean of the block is computed with all the pixels in the block B_j (j = 1, 2, 3, ..., $m \times n$). The calculation of the average of the image block is shown in Equation (5).

$$\bar{x} = \text{round}\left[\frac{1}{m \times n}\sum_{j=1}^{m \times n} x_j^i\right] \tag{5}$$

here x_j^i denotes the ith pixel value of each block B_j (j = 1, 2, 3, …, $m \times n$). The grayscale image is converted into a bitmap image using the mean computed in the equation (3). The pixel value 1 is assigned if the corresponding grayscale pixel is greater than that of the mean and vice versa. The bitmap image generation is shown in Equation (6).

$$y_j^i = \begin{cases} 1, & x_j^i \ge \bar{x} \\ 0, & x_j^i < \bar{x} \end{cases} \tag{6}$$

The mean and the first absolute moment are computed as follows:

$$\alpha = \left|\frac{1}{q}\sum_{x_j^i \ge \bar{x}} x_j^i\right| \tag{7}$$

$$\beta = \left|\frac{1}{m \times n - q}\sum_{x_j^i < \bar{x}} x_j^i\right| \tag{8}$$

where α and β are the mean and absolute moment each block B_j (1, 2, 3, …, $m \times n$). The values of α and β are used to reconstruct the image with the Equation (9).

$$X_j^i = \begin{cases} \alpha, & y_j^i = 0 \\ \beta, & y_j^i = 1 \end{cases} \tag{9}$$

Thus, the reconstructed matrix X is the approximated grayscale image of size $M \times N$. Usually, the size of the blocks is considered to be 4 (i.e., m=n=4). The AMBTC method requires less computational time as compared with the BTC method. Thus, AMBTC is the most opted one in the field of image processing.

IV. THE PROPOSED WATERMARKING SCHEME

The watermarking process involves the techniques of DWT and SVD. It consists of 2 processes such as watermarking embedding process and watermarking extraction process. The various stages in watermarking process is shown in Figure 2.
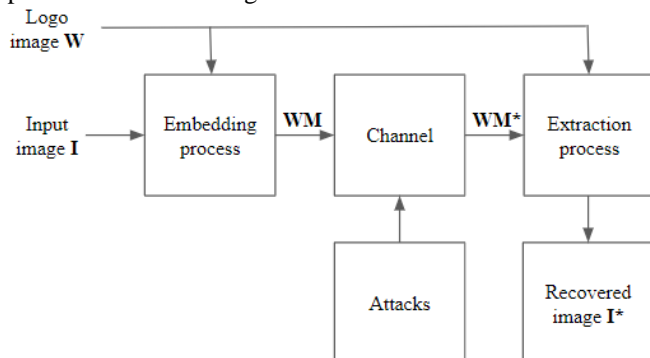

Figure 2. Stages of watermarking process

A. Watermarking Embedding Process

Step 1: The Host grayscale image I of size N × N is applied with one level DWT decomposition using 'Haar' wavelet and four sub-bands such as **LL₁**, **LH₁**, **HL₁**, **HH₁** each of size N/2 × N/2 are obtained.

Step 2: The **HL₁** band of the 1-level decomposed host is chosen, and second level DWT decomposition is applied.

Step 3: The **LH₂** band of the 2-level decomposed image is chosen and the SVD transformation is applied and the matrices U_i, S_i, V_i are obtained.

Step 4: The same process is applied for the logo grayscale image and the SVD is applied for the 2-level decomposed logo. The S-matrix of the logo U_l, S_l, V_l is obtained.

Step 5: The embedding process is done by adding the S-matrices of the images with a weighting intensity α such as $S_w = S_i + \alpha \times S_l$. The resulting S-matrix is embedded in the UV matrix of the host image such as $U_i S_w V_i^T$.

Step 6: The resulting matrix is embedded in the sub-bands of the host image and the inverse DWT is applied to obtain the grayscale watermarked image **WM.**

The various steps in the embedding process of the proposed method is illustrated with the Figure 3. The embedding intensity value is chosen in accordance with the performance of the PSNR of the watermark in the image. These values are shown in the Table 1.
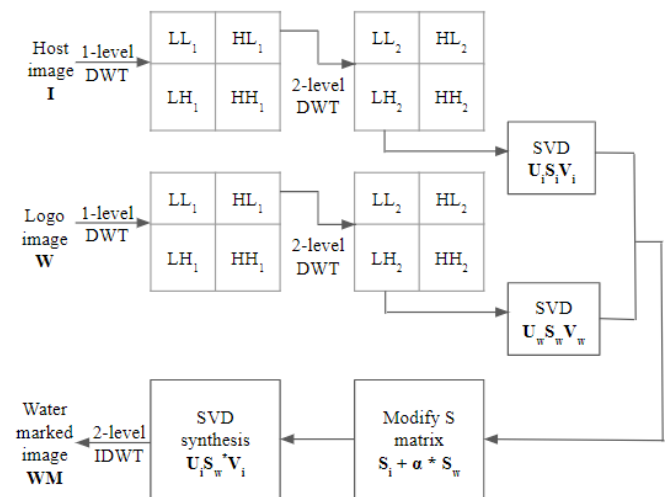

Figure 3. Watermark embedding process

B. Watermarking Extraction Process

Step 1: The 1-level DWT is applied to the watermarked image and the HL₁ band is applied with the 2-level decomposition. The LH₂ band is taken and the SVD transformation is performed and matrices U_w, S_w^*, V_w are obtained.

Step 2: The S-matrix of the embedded logo is obtained by $S_l^* = (S_w^* - S_i) / \alpha$. The obtained S-matrix is embedded with UV matrix of the logo by performing

inverse SVD transformation.

Step 3: The 2-level inverse DWT of the obtained SVD matrix is used to extract the original logo from the watermarked image.

Thus, the watermark extraction process is the reverse process of the watermark embedding process. The flowchart of the extraction process is shown in the Figure 4.
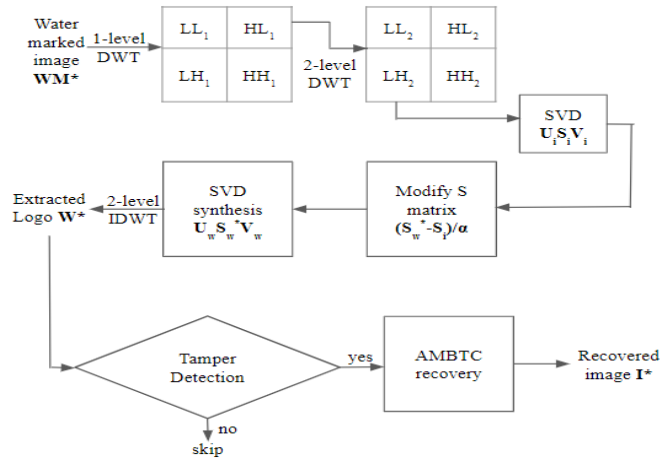

Figure 4. Watermark extraction process

The results of the embedding and extraction process is shown in the Figure 5. The watermarking was implemented in the grayscale images of Lena (Figure 5a) and Airplane (Figure 5b).
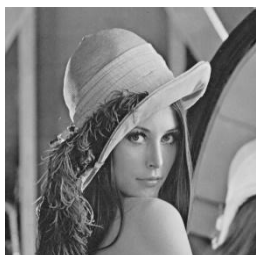

Figure 5a. Host image   **Figure 5b**. Logo image

Figure 5c. Watermarked image   **Figure 5d**. Extracted logo

The embedding intensity is varied in accordance with the PSNR performance of the watermarking process and the values are shown in Table I.

Table I. PSNR(in dB) performance with various embedding intensities.

Embedding Intensity α	PSNR (in dB)
0.05	80.732
0.06	74.960
0.07	71.762
0.08	69.271
0.09	67.464
0.1	66.175
0.2	59.179
0.25	57.063
0.3	55.417
0.4	52.792
0.5	50.817
1.0	44.904
1.25	43.041
1.5	41.507

This Table-I shows various values of the intensity with the respective PSNR performance in embedding the watermark. From the above table, the intensity level $\alpha = 1.25$ is chosen for the embedding process because the PSNR value after the extraction process was good when compared with the other α values.

V. TAMPER DETECTION AND RECOVERY

The extracted logo is used to detect the tampered region in the host image and the regions are recovered using the AMBTC method. The tampered image is divided into 4 x 4 blocks and the tampered region is localized. The untampered pixels are undergone with the AMBTC technique and the average pixel value is estimated for the tampered pixel in the block. Due to the computational simplicity, the evaluation time of AMBTC mean and absolute moment for every block is less as compared with the BTC technique.

VI. EXPERIMENTAL RESULT AND ANALYSIS

The imperceptibility of the watermarked image WM with the original host image I is measured by calculating the PSNR and the similarity between the original logo and the extracted logo is measured by the calculation of the normalized correlation NC shown in the Equation (10).

$$\text{PSNR (I, WM)} = 10 \times \log_{10} \frac{(255)^2}{MSE} \, (dB) \tag{10}$$

The mean square error between the original and the watermarked image is obtained by the Equation (11).

$$MSE = \frac{1}{m \times n} \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} [I(i,j) - WM(i,j)]^2 \tag{11}$$

The normalized correlation between the extracted logo W* and original logo W is obtained by the Equation (12).

$$NC(W,W^*) = \frac{\sum_i \sum_j W(i,j)W^*(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2} \sqrt{\sum_i \sum_j W^*(i,j)^2}} \tag{12}$$

The performance of the proposed scheme between the watermarked image and the host image for PSNR analysis and the extracted logo and the original logo for the correlation analysis with various noises are evaluated and is shown in the Table-II.

Table-II. Performance of PSNR and NC values with various attacks.

Attacks	PSNR (in dB)	NC
Salt and Pepper noise	41.443	0.998
Gaussian noise	37.935	0.997
Poisson noise	48.421	0.999
Speckle noise	36.279	0.996
JPEG compression attack	43.041	0.999

VII. RESULT AND DISCUSSION

Thus, the recovery with the AMBTC technique provides PSNR (in dB) of 35.917 for a salt and pepper noise attacked image with an intensity 10%. The tampered image and recovered image are shown in Figure.6a and Figure.6b, respectively. Also, the method shows that the watermark is robust to JPEG compression attacks.

Figure 6a. Tampered image   **Figure 6b**. Recovered Image

VIII. CONCLUSION

In this paper, a reversible watermarking scheme is proposed with the techniques of DWT and SVD. Thus, the watermark embedded in the host image was robust to the JPEG compression attacks. The recovery was performed by AMBTC method in the tampered region to recover the noise attacked pixels in the tampered region. The PSNR of the recovered image was around 35 dB. So, our future work will depend on the enhancement of the recovery process of the tampered region by preparing an embeddable AMBTC image along with the watermarking.

REFERENCES

1. Singh, A.K. "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images". Multimed Tools Appl 76, 8881–8900 (2017).
2. El Bireki, Majdi & Abdullah, Mohammad Faiz Liew & Ukasha, A. & Elrowayati, Ali. (2016). "Digital image watermarking based on joint (DCT-DWT) and Arnold transform". International Journal of Security and Its Applications. 10. 107-118. 10.14257/ijsia.2016.10.5.10.
3. Ikpyo Hong, Intaek Kim and Seung-Soo Han, "A blind watermarking technique using wavelet transform," ISIE 2001. 2001 IEEE International Symposium on Industrial Electronics Proceedings (Cat. No.01TH8570), Pusan, South Korea, 2001, pp. 1946-1950 vol.3.
4. Swain M., Swain D., Paikaray B.K. (2020) "A Competitive Analysis on Digital Image Tamper Detection and Its Secure Recovery Techniques Using Watermarking". In: Swain D., Pattnaik P., Gupta P. (eds) Machine Learning and Information Processing. Advances in Intelligent Systems and Computing, vol 1101. Springer, Singapore
5. Poonam, Shaifali M. Arora, "A DWT-SVD based Robust Digital Watermarking for Digital Images", Procedia Computer Science, Volume 132,2018, Pages 1441-1448, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.05.076.
6. A. Menendez-Ortiz, C. Feregrino-Uribe, R. Hasimoto-Beltran and J. J. Garcia-Hernandez, "A Survey on Reversible Watermarking for Multimedia Content: A Robustness Overview," in IEEE Access, vol. 7, pp. 132662-132681, 2019.
7. Wang, C. & Zhang, H. & Zhou, X.. (2018). "Review on self-embedding fragile watermarking for image authentication and self-recovery". Journal of Information Processing Systems. 14. 510-522. 10.3745/JIPS.02.0082.
8. N. Dey, D. Biswas, A. B. Roy, A. Das and S. S. Chaudhuri, "DWT-DCT-SVD based blind watermarking technique of gray image in electrooculogram signal," 2012 12th International Conference on Intelligent Systems Design and Applications (ISDA), Kochi, 2012, pp. 680-685.
9. O. Jane, E. Elbaşi, H.G. İlk,Hybrid Non-Blind Watermarking Based on DWT and SVD, Journal of Applied Research and Technology, Volume 12, Issue 4, 2014, Pages 750-761, ISSN 1665-6423, https://doi.org/10.1016/S1665-6423(14)70091-4.
10. S. K. Kapde, Mr. S.V. Patil, "Image compression using BTC and AMBTC", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), Volume 1, Issue 10, December 2012, ISSN: 2277 – 9043
11. C. Kim, D. Shin, C. Yang, "Self-embedding fragile watermarking scheme to restoration of a tampered image using AMBTC", Pers Ubiquit Comput 2018. volume 22, pages 11–22.
12. M. Makbol, Bee Ee Khoo, Taha H. Rassem, "Block-based discrete wavelet transform singular value decomposition image watermarking scheme using human visual system characteristics", The Institution of Engineering and Technology 2015 Image Processing pp. 1–19.
13. J. M. Garcia, R. R. Reyes, V. Ponomaryov, Cl. C. Ramos, "Watermarking Algorithm for Authentication and Self-Recovery of Tampered Images Using DWT", 21-24 June 2016, 9th International Kharkiv.
14. T. Nguyen, C. Chang, X. Yang, "A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain", International Journal of Electronics and Communications (2016), doi: http://dx.doi.org/10.1016/j.aeue.2016.05.003
15. C. Patvardhan, P. Kumar and C. V. Lakshmi, "Robust DWT based color image watermarking scheme," 2015 39th National Systems Conference (NSC), Noida, 2015, pp. 1-6.
16. Radu O. Preda, "Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain", Measurement Volume 46, Issue 1, January 2013, Pages 367-373

17. X. Qi, X. Xin, "A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization", Journal of Visual Communication and Image Representation Volume 30, July 2015, Pages 312-327.
18. Rakhmawati. L, Wirawan. W, & Suwadi. S, "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability", J Image Video Proc. 2019, 61(2019). https://doi.org/10.1186/s13640-019-0462-3
19. Y. Li and L. Du, "Semi-fragile watermarking for image tamper localization and self-recovery," Proceedings 2014 IEEE International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Wuhan, 2014, pp. 328-333.
20. Chin-Feng Lee, Jau-Ji Shen, Zhao-Ru Chen, Somya Agrawal, "Self-Embedding Authentication Watermarking with Effective Tampered Location Detection and High-Quality Image Recovery", Sensors (Basel) 2019 May; 19(10): 2267.
21. Durgesh Singh, Sanjay K. Singh, "Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability", Journal of Visual Communication and Image Representation, Volume 38,2016, Pages 775-789, ISSN 10473203, https://doi.org/10.1016/j.jvcir.2016.04.023.
22. Som S., Palit S., Dey K., Sarkar D., Sarkar J., Sarkar K. (2015), "A DWT-based Digital Watermarking Scheme for Image Tamper Detection, Localization, and Restoration". Advances in Intelligent Systems and Computing, vol 305. Springer, New Delhi.
23. S. Sharma, "A Survey of Blind & Non-Blind Watermarking Techniques", International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016 1218, ISSN 2229-5518.
24. Z. Zhang, C. Wang and X. Zhou, "Image watermarking scheme based on Arnold transform and DWT-DCT-SVD," 2016 IEEE 13th International Conference on Signal Processing (ICSP), Chengdu, 2016, pp. 805-810.

AUTHORS PROFILE

Shaik Hedayath Basha, completed B.E. in Electronics and Communication Engineering, under Madras University in the year 2004, completed M.E. in Applied Electronics specialization at Sathyabama University in the year 2008, completed M.Tech in Digital Electronics and Communication Systems specialization under JNTU – Anantapuramu, Andhra Pradesh, Pursuing Ph.D. in Anna University. I'm having more than 11 years of teaching experience, presently working as an Assistant professor in R.M.K. College of Engineering and Technology. Published more than 7 papers in the reputed International Journals, interested areas of research are Digital Image and Video Watermarking, Digital Image and Video Processing and Cryptography. Memberships: MISTE, MSDIWC.

Vinodh Kumar R is an undergraduate student at R.M.K College of Engineering and Technology under the faculty of Electronics and Communication Engineering. He is a member at ISTE (Indian Society for Technical Education).

Teekaaram V is an undergraduate student at R.M.K College of Engineering and Technology under the faculty of Electronics and Communication Engineering. He is a member at ISTE (Indian Society for Technical Education).

Vishnu N is an undergraduate student at R.M.K College of Engineering and Technology under the faculty of Electronics and Communication Engineering. He is a member at ISTE (Indian Society for Technical Education).

Kamalesh R is an undergraduate student at R.M.K College of Engineering and Technology under the faculty of Electronics and Communication Engineering. He is a member at ISTE (Indian Society for Technical Education).