IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Review on Watermarking Scheme for Digital Image Authentication, Tampering and Self Recovery.

Hiral A. Patel[1*], Dipti B. Shah[2]

[1]Sutex Bank College of Computer Applications & Science, Veer Narmad South Gujarat University, Surat, India
[2]G.H.Patel P.G. Department of Comp. Sc. and Technology, Sardar Patel University, VV Nagar, India

**Corresponding Author: hiral_shreya2003@yahoo.com*

Available online at: www.ijcseonline.org

Accepted: 17/Jun/2018, Published: 30/Jun/2018

***Abstract*—** As the use of internet grows rapidly, there are some of the securities problems arise. Electronic security mechanisms are already followed on Internet even than these problems are increased day by day. This paper discusses the current research trend to solve the issues of digital image authentication and integrity. Different systems suggested by researchers to solve the above mentioned issues are studied and are classified as Fragile watermarking system as well as Semi-fragile watermarking system. Some of the researchers also apply the combination of fragile as well as semi-fragile watermarking system. Individually different systems are analyzed where some systems solve the authentication issue, some systems work with tamper localization where as other systems are there which has capability to get back the original image from the tampered image. Review findings are discussed based on the existing systems discussed by other researchers. Some of the challenges come up based on these reviews and are also discussed here.

***Keywords*—** Digital Watermarking, Image Authentication, Tamper detection, Tamper localization, Self Recovery.

I. INTRODUCTION

The data set on paper is the history now a day because of the digitalization of it. The digital data becomes most popular way for communication between users. Among these documents, digital images are used as legal proof and they can work as agents of secret communication. Before considering any image as legal proof there is a need to test the originality of the image. Image manipulation software is available in the market using which the image can be easily modified. Users may modify the image for their personal benefits in different fields like medical images are manipulated for misrepresentation of patients' diagnosis, journalist modifies image for getting more popularity from readers, before insurance claim, the image is altered so customers can claim for more rewards from company, during crime investigation - image is tampered for getting positive response in court in favor of clients and so on.

As alteration of images increases, it is necessary to test whether the received image is original or manipulated. Means there is a need to test the authenticity and integrity of the original image. Some unintentionally manipulated operations are JPEG compression, Gaussian noise, Salt & Pepper etc. and some intentionally manipulated operations on images are Copy move (Cloning), Image Splicing, Text edition, Object removal, Cropping etc. Unintentional operations are applied on images for easy transmission where as intentional operations are applied for specially misguides the other person. So there is a need to provide security to the images for intentionally manipulated operations. This problem can be solved using active approach named digital watermarking. This active approach requires pre-processing step at the time of capturing image. It embeds the watermark to the image which helps for the authentication of the image.
If the requirements are for authentication then fragile watermarking systems are developed by researchers which never tolerate a single bit modification within the watermarked image. For the content authentication, semi-fragile systems are developed which differentiate malicious (intentional operations) as well as non-malicious (un-intentional operations) attacks during transmission. Semi fragile watermarking technique becomes fragile for malicious operations where as robust with non-malicious operations. It allows the content preserving operations and finds out the tampering applied on watermarked image. If the image is tampered then the originality of the image is destroyed so this image becomes useless. There are some systems designed which find out the regions where the tampering was applied and some systems are also tried to recover the original image from the tampered watermark image.

Lots of research work is conducted till date in this direction still now a day researchers try to enhance the existing systems by implementing different approaches.

In this paper, the reviews of research papers are discussed in Section-2. Section-3 explains the review finding and section-4 lists out the challenges found during the study and Section-5 discusses conclusion.

II. RELATED WORK

The researchers are worked under the issues of digital authentication and tampering. They solved above problems using two different watermarking techniques named Fragile and Semi-Fragile watermarking. The reviewed research papers are classified within these two categories and are discussed below:

2.1. FRAGILE WATERMARKING SYSTEM:

The fragile watermarking system embeds the watermark within image in such a way that it doesn't tolerant a single bit modification in watermarked image. D. Vaishnavi et. al. [1] used two different images- one is cover image where as another is watermark. The system generated watermark using canny edge detection and Arnold transform was applied for scrambling watermark. This watermark embedded into the LSB part of the image. By implementing the system, PSNR was achieved up to 50.6246dB and NCC was achieved up to 0.9972. XOR operation was used for embedment and extraction process. They tested their system for attacks like Copy Move attack, text edition, Image splicing and object removal. Woo Chaw Seng at. al. [2] proposed first level of DWT technique and apply watermarking in LL. Image was divided into numbers of blocks and the watermark was embedded in 6th bit of each block. By implementing this proposed algorithm, they observed that the algorithm survived with content preserving operation like JPEG compression upto 85%. Dadkhah Sajjadet. al. [3] generated two watermarks one for tamper recovery (3 bits per block) which was generated by applying 4X4 blocking and SVD on image and another authentication watermark (12 bits per block) was generated which contains the primary location information of each block of image. The tamper related watermark was embedded in LSB plane and another watermark was embedded in SB plane. They tested collage attack and VQ attacks for testing of tampering. They implemented system on color image and above mentioned tasks were performed for each color matrix. Behrouz Bolourian Haghighi et. al. [4] prepared blind fragile watermarking system for color as well as gray scale images in which the watermarks were generated from the original image. First watermark generated using Lifting Wavelet Transform (LWT) and then to reduce the bit error LSBrounding method used. Another watermark generated by applying halftoning of image using Stucki kernel. The scrambling was applied to both watermarks using shifting bits. The watermark embedded in 2nd LSB part. The system tested by applying splicing and copy move attacks to the image and they achieved the imperceptibility up to 46dB. The suggested system destroyed the watermark even with the image preserving operations like JPEG compression, Gaussian noise etc. Cheonshik Kim et. al. [5] generated two watermarks by applying 4X4 blocking. First watermark generated by calculating average from block values and converted image into binary by comparing each values with average values of blocks. If value was greater than average value than it was considered as 1 otherwise 0. Another watermark generated by calculating maximum and minimum values based on first watermark and these two values converted to binary code. These two watermarks were embedded into LSB and 2LSB of original image. The system achieved the PSNR upto 35dB and system was tested for image splicing and cropping. Sawiya Kiatpapan et. al. [6] generated two watermarks by resizing the image with 512X512 and 128X128 and then converted the images into binary form. These two watermarks were embedded in LSB plane of the original image by changing the position of watermark bits. To the destination place, the two watermarks extracted and the sum of absolute difference (SAD) calculated for images. If any change found then from the two watermarks the tampered area was filled. The system was tested with image splicing only. Authors stated that their system will not work properly if the watermarks will damage. D. Vaishnavi et. al. [7] used two different files named cover and watermark image. To generate the watermark, authors used DWT. The watermark image divided into high and low frequency, using threshold value, the high frequency image divided into binary image. To embed the watermark, first Arnold transform applied on host image. Image divided into 2X2 blocks and binary watermark was embedded at first value of each block. Again inverse Arnold transform applied on image to get watermarked image. Here LSB plane used for embedment. To test the image, original watermark and extracted watermark compared using XOR. If difference found means image was tampered. The imperceptibility achieved up to 64dB. The system tested with copy move, image splicing, text edition and object removal. Sanjay Rawat et. al. [8] also used another file as a watermark. The logistic map calculated from this image and it used as a watermark. The scrambling applied to the original image using Arnold transform (multiple times – k). Then in LSB plane of this scrambled image, the watermark embedded using XOR operation and again the reverse scrambling applied. To check the tampering, the embedded watermark extracted and compared with the original file. If not matched then it considered as tampered image and it also suggested the region where the tampering applied. When the system tested with different images then the PSNR value achieved up to 50.72dB. Also for tampering testing, Copy move, Image splicing, text edition, object removal, collage all attacks applied one by one and results were observed. Marco Botta et. al [9] mainly focused on special attack which may be possible during transmission related with fragile transformation. As per

authors' observation, it is possible to tamper the watermarked image easily when watermark is embedded in LSB plane of image and when another file is used as watermark. As per their discussion, takes the watermarked image and stores the LSB plane's values in one matrix (L) then applies tampering on watermarked image. Now replace the LSB plane of the tampered image with the matrix (L). So the image is tampered and watermark is not changed. They tested this by tampering image with 50% tampering as also with 100% tampering, in both cases the watermark extracted as it is and it didn't show that the image was tampered. They suggested that when the watermark was embedded in LSB plane then there should be some authentication code need to generate based on other 7 planes which help in identifying the tampering. Sergio Bravo-Solorio et. al. [10] tried to improve the scheme given by Mr. Zhang and Wang. The proposed system generated reference code by scrambling image's 5 MSB planes using permutation and two different secret keys. Then these two codes combined with each other. The description code generated by applying 8X8 blocks of the image and prepared the code using number of row, number of column and index number. The cryptographic hashing applied on 5 MSB planes of each block. The authentication code was generated by applying XOR operation between reference code and description code. The embedment was done in last 3 LSB planes. As per the tested results of the system, 34.6 dB PSNR is achieved and the system gave good retrieval results with cropping, object removal and image splicing.

2.2. SEMI-FRAGILE WATERMARKING SYSTEM:

Semi-fragile watermarking system embeds the watermark in such a way that it works as robust when unintentional manipulations like JPEG compression, Gaussian noise, Salt & Pepper etc. are performed during transmission of image where as it works as fragile when intentional manipulations like text addition, object removal, object addition etc. are performed during transmission. S.S.Sujatha et. al. [11] generated using DWT. Scrambling was applied for providing more security. Watermark embedded in cover image. Different attacks were tested like JPEG compression, Gaussian Noise, salt and pepper. The proposed system was developed only for checking the authentication of image but no work was done for tampering. Buddhika Madduma et. al. [12] generates watermark using feature extraction with Zernike Moment Megnitude (ZMM) method. The system also applied quantization on it. They also generated another watermark using sobel edge map for tamper localization and embeded both watermarks into HL2 and LH2 of DWT. They used Euclidian distance to check the manipulation. They also checked same algorithm for gray and color images. Chitla Arathi [13] presented block based SVD transformation method. Her proposed technique was non-blind watermarking system. She tested system by applying Gaussian noise, Resizing image and JPEG compression. Chaitanya Kommini et. al. [14] generated watermark using DWT and by adding the values of HH2, HL2 and LH2. The algorithm also generated secret key for providing security using logistic map. The system embedded watermark into original image in HL1 and LH1 sub-band of original image by applying blocking of 2X2. The proposed algorithm identified the tampered region from tampered image. The algorithm implemented only for the gray scale image. Lintao L.V. et al. [15] generated watermark using 3-level Haar DWT and using logistic map the random number generated using LL3. The original image scrambled using Arnold and applied block based DCT. The mid bend was selected to embed the watermark and use Zig-zag method for it. After implementing the algorithm authors achieved the result upto 44.2936 dB. U.M.Gokhale et. al. [16] generated chaotic sequence using Logistic Map for scrambling the original watermark which was considered as secret key. They also applied threshold value and xor operation for scrambling. The proposed system was based on Integer DWT, SVD. They applied first level DWT and performed SVD for each sub band. The singular value of scrambled watermark embedded using scaling factor to each sub band. The proposed system was non-blind watermarking technique as original image used to extract. They used the chaotic sequence to extract the original watermark. They achieved result without attack was PSNR value with 50.4488 and NC value with 1. N. Chunlei Li et. al. [17] have mainly focused on authentication and self recovery of face. The proposed system generated 2 bits information watermark using 16X16 block, PCA and eigen face coefficients. The system also generated 3 bits authentication code from each blocks using SVD and Eigen values. The watermark encrypted by combining 2 and 3 bits code than apply permutation using Secret key. This watermark embedded using 2nd level DWT of each block and embedded in HL2, LH2 and HH2 sub band. The system achieved imperceptibility result upto 53.3. The tempered portion checked and it recovered using the system. Javier Moina et. al. [18] embedded three watermarks within image in which one used for authentication where as other two used for self recovery. The watermarks generated using sub sampling of image, halftoning and edge detection techniques. The DWT transform was used for embedding of watermark. They achieved PSNR upto 35 dB. Their system was robust against JPEG compression with 75% compression with 32 dB and was able to recover tampered image. Gadhiya Tushar D. et. al. [19] have worked with medical radiography images. Three hashed images prepared which prepared by applying canny edge detection on LH, HL and HH sub-band of DWT of original image. These images used to the destination place for the verification of the original image so the given system was the non-blind technique. The content preserving operations like brightness, gamma correction, JPEG compression tested. Average edge index used to test two hashed matrices. Ramos Clara Cruz et. al. [20] generated digital signature by applying 16X16 blocking.

For embedment they used LL sub-band of DWT of original image. The JPEG compression and Gaussian noise was tested. The algorithm is tested with gray and color both type of images. Archana Tiwari et. al. [21] used new file as a watermark and original file as cover. Two watermarks used among these one used for robustness and another used for semi-fragility. To embed the watermark, the system applied 4X4 blocking of original file, calculated vector quantization and variance. They embedded the watermark based on the threshold value. They tested the system with different gray scale images and achieved the PSNR up to 41.79dB. Also the system tested by applying image preserving operations like blur, Gaussian, Salt & Pepper, JPEG compression and filtering where as intentionally manipulated operations like cropping, text edition.

2.3. OTHER SYSTEMS:

Researchers also work under the same issue and try to solve the issue using different approaches. Chetan K. R. et. al. [22] generated watermarks based on the required region of original image. The color image converted in gray image and image divided into 128X128 block and based on gradient binaries of each block, they classified re-generatable and non-regeneratable content and then applied semi-fragile and fragile technique respectively. Tampering was tested using copy move, splicing and object removal attacks. V. Kavitha et. al. [23] generated watermark using DWT and performed permutation for more security. The watermark embedded using Reed Solomon encoding technique which is used in digital communication channel. The system tested by tampering the image by adding new object in original file (Image splicing). Wan-Li Lyu et. Al. [24] worked for color image tampering. The suggested system calculated the alpha channel plane based on the feature of the original image by calculating mean on 2X2 non-overlapping blocks. They used hashing technique and prepared HAT (hash address table) and the hashing was applied based on pixel position not based on pixel intensity value. They used Shamir's algorithm for doing this. The color PNG file created from the original and alpha plane. The alpha channel plane forwarded with the original image which used to the destination place for authentication of original image. The system tested for image splicing and text addition.

III. REVIEW FINDINGS

Lots of research work is done for the issue of authentication, tamper detection, localization and self recovery. As discussed earlier, some systems are based on fragile watermarking systems where as some systems are based on semi-fragile watermarking systems.

Based on the reviews of fragile watermarking systems, all the systems tries to solve the authentication as well as tamper localization where as [2, 3, 4, 5, 6, 10] systems also tries to retrieve the original image from tampered one. [1, 4, 5, 7, 8, 10] systems are developed for gray scale image and [2, 3, 4, 6] are for color image. To implement the system, researchers used two different files named cover image and watermark image [1, 7, 8, 9]. With these types of systems, the tampered region can be found properly but the self recovery is difficult. Other systems generated watermark by extracting features of the original image using different methods like SVD, LWT, Halftoning, by applying non-overlapping blocking and then performing operations like minimum, maximum, mean etc. on each block. To provide more security to the watermark image, scrambling is applied using Arnold Transform, Permutation and shifting top to bottom rows and columns [1, 4, 5, 7, 10]. Embedment of watermark with these systems is normally done using spatial domain LSB method. Directly the one or more image planes of bits are replaced with the watermark image. The imperceptibility of the watermarked image which is measured as PSNR is achieved up to 64.18 dB [7] within systems. But the systems which has capability of self recovery are achieved PSNR up to 46 dB [4]. Systems which are designed using fragile watermarking are normally of blind watermarking system means during extraction process original image is not required. Because these systems are fragile system so it treats in same manner with content preserving operations and tampered operations. These systems were mainly focused with tampered attacks like copy move attack [1, 4, 7, 8], text addition [1, 7, 8], object removal [1, 7, 8, 10], collage attack [3, 8], cropping image [2, 5, 10] and image splicing [1, 4, 5, 6, 7, 8, 10]. Researchers of [9] claimed that the system which embeds the watermark in LSB planes of the original image can easily tampered without affecting the watermark.

Based on the reviews of semi fragile watermarking systems, all the systems tries to solve the authentication, [12, 14, 15, 17, 18, 19, 21] systems identifies the tampered region among these [15, 17, 18] systems also retrieve the original image from tampered one. Major systems are developed for gray scale image and [20] system is designed for color image. To implement the system, researchers used two different files named cover image and watermark image [13, 16, 21]. With these types of systems, the tampered region can be found properly but the self recovery is difficult. Other systems generated watermark by extracting features of the original image using different methods like DCT, DWT, Canny and Sobel edge detection techniques, SVD, PCA, Halftoning etc.. To provide more security to the watermark image, scrambling is applied using Arnold Transform and Logistic map [11, 14, 15, 16]. Embedment of watermark with these systems is normally done using frequency domain methods like DCT, DWT or the combination of these two, vector quantization etc.. Some of the systems also apply non-overlapping blocking of size 2X2, 4X4 or 8X8 and then embed the watermark. The imperceptibility of the watermarked image is achieved up to 59 dB in [11] but this system works only for authentication not for tampering. But the systems which has capability of self recovery are

achieved PSNR up to 53 dB [17]. Among these systems, [13, 16, 19] systems are based on non-blind watermarking systems which require original image to the destination for extracting watermark where as other systems are blind watermarking systems. Semi fragile watermarking system has capability to differentiate intentionally as well as unintentionally manipulated operations. The researchers were tested image preserving operations like JPEG compression, Gaussian noise, Salt & Pepper noise etc. and their systems became robust with these operations and became fragile with tampered attacks. Tampered attacks like copy move attack [14, 17], text addition [12, 14, 21], object removal [12, 15, 18], cropping image [21] and image splicing [12, 14, 15, 18] are tested by the systems to achieve results. To design a system with semi-fragile watermarking system is more difficult than the fragile system. But if we compare these two types of systems then semi-fragile system is better than fragile system because of its malicious and non malicious attack differentiation.

IV. RESEARCH GAP

Based on above findings some of the research gaps identify which are listed below:

- Less work was conducted for color image.

- Imperceptibility of watermarked image for fragile watermarking system is up to 64dB with tamper localization and up to 46dB with self recovery which needs improvement. The same for semi-fragile watermarking system is up to 59dB where as 53dB with self recovery.

- With fragile systems minor modification destroys the watermark. These systems are not concerned about the content of the image so they may be failed with tamper recovery so system needs some enhancement.

- When the watermark is embedded into LSB planes then without affecting the embedded watermark, the original image can be tampered [9] then this tampering is difficult to identify.

- Tampered region is not perfectly identified as well as recovered with minor modification.

- Many systems are designed to test tampering but researchers tested some of the attacks it may be possible that for other attacks their system may not give proper outputs.

V. CONCLUSION

Authentication and tampering are the e-security issues which can be solve using watermarking techniques. Fragile as well as Semi-fragile watermarking techniques are helpful to solve these issues. It is easy to extract the watermark from watermarked image with fragile system where as it is difficult with semi fragile system. With tampering issue, fragile system is less robust than semi-fragile system because watermark embedment is applied directly on one of the bit plane of image so it is easy to modify watermarked image without affecting embedded watermark. Also fragile system can't differentiate the intentional and non-intentional manipulation operations and it treats both in a same manner whereas semi-fragile system can differentiate intentional as well as un-intentional manipulations. With pros and cons, both the watermarking systems (Fragile and Semi-fragile) can solve the problem of authentication and integrity.

Lots of systems are designed to solve the issue of authentication and tampering for gray as well as color images. There is a scope to develop the model which will be based on the semi-fragile watermarking system for color image to improve the imperceptibility of watermarked image and recovery of original image. The model will generate the watermark by extracting the features of the original image which will help to retrieve the original image from the tampered image to enhance the performance of the existing systems.

REFERENCES

[1]. Vaishnavi D., and T. S. Subashini. "Image Tamper Detection based on Edge Image and Chaotic Arnold Map." Indian Journal of Science and Technology vol. 8, No. 6: pp. 548-555, 2015.

[2]. Pongsomboon, Paween, Toshiaki Kondo, and Yoshiyuki Kamakura. "An image tamper detection and recovery method using multiple watermarks." Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 13th International Conference on. IEEE, 2016.

[3]. Dadkhah, Sajjad, et al. "An effective SVD-based image tampering detection and self-recovery using active watermarking." Signal Processing: Image Communication Vol. 29, No.10 : pp. 1197-1210, 2014.

[4]. Haghighi, Behrouz Bolourian, Amir Hossein Taherinia, and Ahad Harati. "TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique." Journal of Visual Communication and Image Representation, 2017.

[5]. Kim, Cheonshik, Dongkyoo Shin, and Ching-Nung Yang. "Self-embedding fragile watermarking scheme to restoration of a tampered image using AMBTC." Personal and Ubiquitous Computing Vol. 22 No. 1: pp.11-22, 2018.

[6]. Kiatpapan, Sawiya, and Toshiaki Kondo. "An image tamper detection and recovery method based on self-embedding dual watermarking." Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2015 12th International Conference on. IEEE, 2015.

[7]. Vaishnavi, D., and T. S. Subashini. "Fragile watermarking scheme based on wavelet edge features." Journal of Electrical Engineering & Technology Vol. 10 No.5 : pp. 2149-2154, 2015.

[8]. Rawat, Sanjay, and Balasubramanian Raman. "A chaotic system based fragile watermarking scheme for image tamper detection." AEU-International Journal of Electronics and Communications Vol. 65 No.10 : pp. 840-847, 2011.

[9]. Botta, Marco, Davide Cavagnino, and Victor Pomponiu. "A successful attack and revision of a chaotic system based fragile

watermarking scheme for image tamper detection." AEU-International Journal of Electronics and Communications Vol. 69 No. 1 : pp. 242-245, 2015.
[10]. Bravo-Solorio, Sergio, et al. "Fast fragile watermark embedding and iterative mechanism with high self-restoration performance." Digital Signal Processing Vol. 73 : pp. 83-92, 2018.
[11]. Sathik M. M., and S. S. Sujatha. "Authentication of digital images by using a semi-fragile watermarking technique." International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2 No. 11 : pp. 39-44, 2012.
[12]. Madduma Buddhika, and Sheela Ramanna. "Content-based image authentication framework with semi-fragile hybrid watermark scheme." Man-Machine Interactions 2. Springer Berlin Heidelberg, pp. 239-247, 2011.
[13]. Arathi Chitla. "A semi fragile image watermarking technique using block based SVD." International Journal of Computer Science and Information Technologies Vol. 3 No. 2 : pp. 3644-3647, 2012.
[14]. Kommini Chaitanya, Kamalesh Ellanti, and E. Harshavardhan Chowdary. "Semi-Fragile Watermarking Scheme based on Feature in DWT Domain."International Journal of Computer Applications Vol. 28 No. 3 : pp. 42-46, 2011.
[15]. LV LINTAO, et al. "A semi-fragile watermarking scheme for image tamper localization and recovery." Journal of Theoretical and Applied Information Technology Vol. 42 No. 2 : pp. 287-291, 2012.
[16]. Gokhale U. M., and Y. V. Joshi. "A semi fragile watermarking algorithm based on SVD-IWT for image authentication." International Journal of Advanced Research in Computer and Communication Engineering Vol. 1 No. 4, 2012.
[17]. Li Chunlei, et al. "Semi-fragile self-recoverable watermarking scheme for face image protection." Computers & Electrical Engineering on Elsevier ,2016.
[18]. Molina-García, Javier, et al. "Watermarking algorithm for authentication and self-recovery of tampered images using DWT." Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW), 2016 9th International Kharkiv Symposium on. IEEE, 2016.
[19]. Gadhiya, Tushar D., et al. "Use of discrete wavelet transform method for detection and localization of tampering in a digital medical image." IEEE Region 10 Symposium (TENSYMP), 2017. IEEE, 2017.
[20]. Ramos, Clara Cruz, et al. "Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Domain." Discrete Wavelet Transforms-Algorithms and Applications. InTech, 2011.
[21]. Tiwari, Archana, and Manisha Sharma. "An Efficient Vector Quantization Based Watermarking Method for Image Integrity Authentication." Progress in Intelligent Computing Techniques: Theory, Practice, and Applications. Springer, Singapore, pp. 215-225, 2018.
[22]. Chetan, K. R., and S. Nirmala. "Intelligent Multiple Watermarking Schemes for the Authentication and Tamper Recovery of Information in Document Image." Advanced Computing and Communication Technologies. Springer, Singapore, pp. 183-193, 2018.
[23]. Kavitha V., and Subhashree M. "Detection and tampering of Tampered Images." International Conference on Current Research in Engineering Science and Technology (ICCREST): pp. 57-61, 2016.
[24]. Lyu, Wan-Li, Chin-Chen Chang, and Feng Wang. "Color PNG Image Authentication Scheme Based on Rehashing and Secret Sharing Method." Journal of Information Hiding and Multimedia Signal Processing Vol. 6 No. 3 : pp. 523-533, 2015.
[25]. Mishra Mitali, and Flt Adhikary. "Digital image tamper detection techniques-a comprehensive study." International Journal of Computer Science & Business Informatics Vol. 2 No. 1: pp. 1-12, 2013

Authors Profile

Ms. Hiral Patel pursed M.C.A., M.Phil and currently pursing Ph.D. from SPU, VV Nagar, Gujarat. She has cleared GSET exam which was held in August 2017. She is currently working as Assistant Professor at Sutex Bank College of Computer Application and Science, Surat. She has 17 years of teaching experience. Her area of interest is in Electronic Security, Image Processing and Networking.

Dr. Dipti Shah pursed M.C.A. and Ph.D. in Computer Science. She is currently serving as Professor and Director in Post Graduate Department of Computer Science since 1989. She has published more than 30 research papers in National Journals as well as more than 80 in International Journals. 10 Ph.D students have completed their research work under her and 4 students are currently pursing. Her area of interest is in Computer Graphics, Image Processing, Decision Support System, Artificial Intelligence and Medical Informatics.

