ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Local Binary Pattern (LBP) of Image Tampering Fragile Watermarking Algorithm

Kodavanti Venkata Pratyush
Department of CSE,
Gitam University,
Visakhapatnam, AP, India.

Abstract

In this paper we portray a novel advanced image watermarking strategy utilizing local binary patterns (LBP). Local binary patterns are known for their hearty surface portraying capacities and advanced watermarking utilized as a part of demonstrating the responsibility for sight and sound substance. In this work we propose a LBP union or backwards LBP coordinating procedure and its appropriateness to advanced image watermarking. LBP combination prepare changes to the area pixels values, so that the LBP processed from these pixels is the esteem we need to blend. This procedure considers the prerequisites of an advanced image watermarking, for example, indistinctness and vigor to watermark evacuation assaults. In view of the way of LBP combination it is required that exclusive couple of pixels of a given piece are adjusted to insert watermark. The recreation comes about demonstrate that the strategy is strong to JPEG pressure, revolution and scaling assaults. This LBP union process could likewise be utilized to watermark sensor information for demonstrating the proprietorship. We are sure that this work would prompt another exploration heading in verification of advanced substance.

Keywords: ***Fragile watermarking; Least Significant Bit (LSB); Local Binary Pattern (LBP); Tampering; Texture.***

I. Introduction

Because of the improvement of image processing and information technology, the security of information has pulled in light of a legitimate concern for the analysts in the course of the most recent decade [1]. In this we proposes conspire we utilized a delicate image watermarking plan with recuperate capacity taking into account local binary patterns (LBP). The local binary example administrator is used to extricate localized spatial elements. A local binary example is utilized to speak to the localized relations of a pixel with its neighborhood pixels. Each pixel is measured by the LBP administrator and acquired its own local binary example as representation of local spatial relations. We use the LBP administrator to create confirmation information which are installed into every image hinder with 3 × 3 pixels measure for alter recognition and recuperation. The recovery of information is given by computing the mean estimation of every image square, and after that the mean esteem is changed over into a binary string which is inserted into eight neighboring pixels' LSBs of every image hinder for image recovery. In the proposed method we can take the contribution as 256 × 256 and in addition 512×512 measurement image, one of the favorable position contrasts with other existing framework is that it can likewise handle the shading image. The quality is figured by the PSNR. However in the proposed plot PSNR at all most successful points indicate is likewise computed to show signs of improvement result. The

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

achievement of Internet and computerized customer gadgets, for example, versatile, portable PC, tablet and so on which are utilized by people significantly changes our everyday lives and society. These worries have ended up issues in numerous areas, for example, video and music industry and so on. So as an answer computerized watermarking is mostly utilized. Subsequently computerized watermarking turns out to be extremely shocking examination point.

Computerized watermarking technology that distinguish and make undetectable markings, which can be utilized to find the root, exactness, and approved utilization of advanced information. In future the real improvement of advanced watermarking resemble as: privateer following, image verification, replicating security, copyright insurance, and shroud information. [1][3] The importance of strength is in which watermark is proficient to oppose a few changes in the watermark installed flag. So the decent calculation ought to be strong. As far as the information field computerized, watermarking are grouped into two classification spatial space and recurrence area watermarking. In spatial space technique watermark is insert by adjusting the pixel estimations of novel image and change space handle which implant the information by regulating the change zone coefficients. Semi delicate spatial space strategy is more hearty than recurrence area procedure.

II. Related Work

Watermarking is the way toward implanting computerized motion in the advanced information. Bunches of works have been in the field of watermarking and in this area we will talk about watermarking. I. J. Cox and Matt L. Mill operator laid out some attractive attributes of computerized watermarks. The attributes are as Robustness; Watermark ought to be hard to notice, Tamper resistance, Bit rate, Modification and various watermarks and versatility. I.J. Cox and Matt L. Mill presented a numerical structure which is utilized for investigating some watermarking procedures. They have made an audit of some suggestion for watermarking and endeavored to find qualities and deficiencies [1]. F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn concentrated on information covering up and steganography. They have considered an extent of usages in their survey.

They depicted different ambushes on information covering systems and a gadget StirMark [2]. Jun-Dong Chang, Bo-Hung Chen and Chwei-Shyong Tsai proposed LBP based sensitive watermarking technique with recover limit. Their technique utilizes the LBP director to create acceptance information. They figured the watermark from the photo itself. They have figured confirmation information in perspective of the run of LBP. The affirmation information is w1 and w2 bits, S vector and M vector. Which are embedded into each photo hinder with 3×3 pixels estimate for modify distinguishing proof and recovery. The recovery information is obtained by finding out the mean of piece, and a while later the mean quality is changed over into a twofold string which is embedded into eight neighboring pixels' LSBs of each photo deter for picture recovering. Since the watermark is emerged into the 2-LSBs of pixels of each photo deter, the straightforwardness of watermarked pictures stays better. Jung Dong's strategy is having awesome result for picture adjust disclosure and recovery as appear differently in relation to Zhang's watermarking scheme[3].

T. Ojala, M. Pietikhenl and D. Harwood managed surface gathering. They have evaluated the execution of some surface measures. The creation measure has been adequately used as a piece of different applications. They have proposed some surface measures like Gray Level Difference Method, Texture Measures, Center symmetric Covariance Measures and Local Binary Patterns. A piece unit (TU) is addressed by eight parts, and the surface unit is having the qualities like 0 ,1 or 2 and procured from the square of 3×3 . The total possible arrangement units are 6561 depicting the three level cases in 3×3 bit of pixels.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

III. Local Binary Patterns (LBP)

Ojala introduced LBP operator which considers the 3x3 neighbourhood of each pixel in a given image, and each neighboring pixel is threshold with respect to the center pixel value $I_c(x,y)$ and finally the result is taken in binary form[4]. The center pixel value is replaced by the decimal equivalent of that binary number to form the LBP image.

Here the number of neighbourhood pixels are represented by 'P' and radius of the neighbourhood is represented by 'R'. The LBP operator can be described as in following figure 1. LBP operator is by definition invariant against any monotonic transformations of the gray scale, i.e. as long as the order of the gray pixel values in the image stays the same, the output of the LBP_R operator remains same. A local binary pattern is called uniform if it contains at most two bitwise transition from 0 to 1 or vice versa.

Decimal form of a binary string for the pixel I_c is calculated by the following equation

$$LBP_R^P(I_c) = \sum_{n=0}^{P-1} s(I_n - I_c)2^n \quad (1)$$

Where I_n and I_c are the values of neighbouring and center pixels respectively. The threshold function is given as

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x<0 \end{cases} \quad (2)$$

IV. LBP Synthesis

LBP synthesis or inverse LBP mapping is the reverse of LBP computation process. Given a LBP bit pattern to be embedded in to the data or image, the surrounding pixels of the center pixel are modified such that the computation of LBP on the modified block results in the same pattern synthesized.

For the image processing applications the objective is to synthesize a given bit pattern, for each bit of the LBP modify the corresponding image pixel values such that the thresholding condition is satisfied.

If the one of the bits in the bit pattern to be synthesized is '1' then the corresponding neighborhood pixel value is modified such that it is larger than the center pixel by an amount equal to threshold value to satisfy the thresholding criteria. For embedd bit '0' the neighborhood pixels value is reduced by the threshold values, so that during the computation of the LBP it results in '0' after magnification.

$$If \ \ wm\_bit==1$$
$$I_n=I_c+\Delta$$
$$else$$
$$I_n=I_c-\Delta$$

The value of threshold is chosen to satisfy the imperceptibility criteria of the image watermarking. A larger threshold means larger variation in the neighboring pixels, resulting in degradation in image quality but at the cost increase in watermark extraction errors.

V. Image Watermarking Using LBP

Digital image watermarking procedure involves embedding or hiding a set of bits that represents the owner of the content in an image with negligible impact on the quality of the image. For a better user experience the changes must not be perceptible to the end user. These embedded watermark bits are again extracted from the image to prove the right owner of the content. This extraction must be robust to several intended and unintended manipulations that happen on the watermarked image.

Intended watermark removal attacks include rotation, scaling, translation, filtering etc. and unintended attacks include image compression. The given image is divided into multiple non-overlapping blocks of size NxN and a fixed number of these NxN blocks are grouped to form a group. There could be 'M' such groups. The mapping of NxN blocks to grouping can be linear or random. The same mapping is used during watermark extraction. Randomly grouping NxN blocks helps in improving the secrecy as well as robustness. Each of these groups are used for watermarking either a 8-bit byte or a 16-bit word. If the number of NxN

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

blocks within a group are high then the extraction could result in less number of bit errors, but it reduces the embedding capacity and viceversa. Given a set of bits to be embedded, we use LBP synthesis process to embed these bits into non-overlapping blocks of a given image.

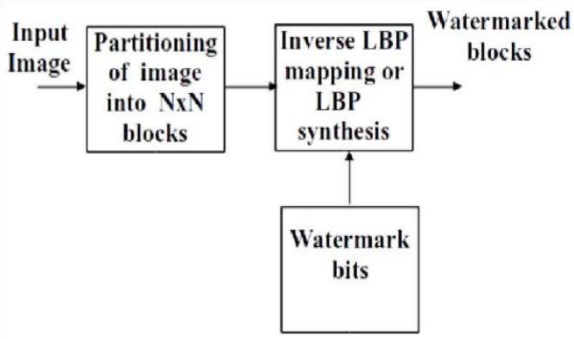


Figure 1. Watermark embedding process.

Watermark Embedding Process

Convert a given watermark bit stream into series of bytes or 16-bit words based on the size of block, each byte or a 16bit word is used for embedding in K number of NxN blocks using LBP synthesis process. During the LBP synthesis, for each watermark bit within the corresponding 16-bit word, 16-pixels in the NxN block are modified such that, the LBP value computed on this modified NxN block results in the synthesized watermark byte or word. We will repeat this process for all the 'M' watermark bytes or 16-bit words for embedding them in to 'M' groups. The modified NxN blocks together make up the watermarked image. If required all the three channels in a color image can be used for watermarking for improving the embedding capacity. The general block diagram of the watermark embedding is shown in figure 1 and block wise embedding process is shown in figure 2

In another LBP based watermarking method we propose to use number of bit transitions in the LBP bit pattern to embed a bit of watermark. In this method, for each bit of the watermark we check if the number of transitions are less than a threshold T_1 and change the pixel values such that the number of transitions in the LBP pattern is as required. In our simulations, we used the number of transitions for bit '1' to be less than or equal to four and for bit '0' the number of transitions set to be more than four for a 8-bit watermark. This method particularly useful in maintaining the quality of the image as the pixels inherently have values that result in fewer transitions required for the watermarking criteria. Especially for images, the neighboring pixels have similar intensity values. Hence we are required to modify only few pixels out of eight for 8-bit watermark at maximum four.

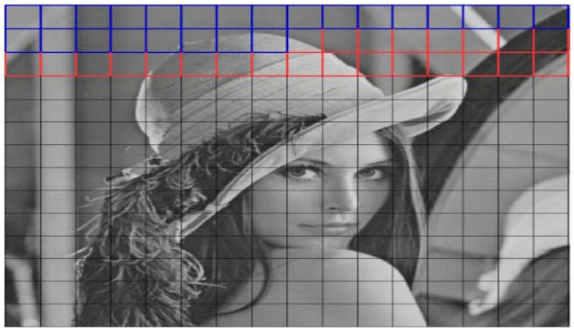


Figure 2. All the K-Blocks in the group are watermarked with same word.

1) Imperceptibility: As the pixels values are changed to obtain LBP that matches the watermark bit pattern, these changes could be visible due to the nature of LBP calculation. When the surrounding pixel values are in huge difference with the center pixel, the change required to match the LBP is very high and these changes could affect the quality. But due to inherent nature of the images, intensity values of nearby pixels, does not vary significantly helping in maintaining the quality of the images, after watermarking. To alleviate this we propose to evaluate the impact of the LBP synthesis on the quality of the image. If the changes required for synthesis are high enough to degrade the quality we discard that NxN block for watermarking. As the watermark is redundantly added to the K blocks it still can be recovered.

Watermark Extraction Process

Given a watermarked image, it is divided into NxN blocks and M groups as its done during watermark

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

embedding process. The blocks are assigned to groups in the similar way as is done during the watermark embedding. During the extraction process, for each group of NxN blocks, LBP values are computed and stored. Histogram of the LBP values obtained for each group of NxN blocks is computed separately. The bin number which has the highest count is noted. This binary number and the equivalent LBP pattern is the actual watermark value which is embedded as a byte or a 16-bit word. For example, if the count of the bin 211 is large compared to all others, the watermark pattern extracted is 11010011. This is similar to majority voting. This way all the groups are processed to extract the complete watermark. The block diagram of extraction of watermark from the watermarked image is shown in figure 3.

For increased robustness of the method error-correction codes can be used on the watermark bits. If the K is smaller then a large number of watermark bits can be added to the image increasing the embedding capacity significantly.

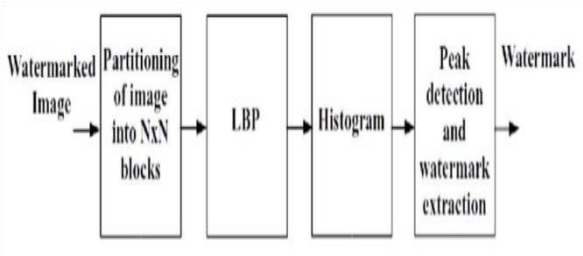


Figure 3. Watermark extraction process.

VI. Proposed Methodology

Local Binary Pattern (LBP) is a feature which is used for classification in digital images. LBP was first elaborated in 1994. Since then it is used as a powerful feature for texture classification. Earlier LBP operator is widely used in texture classification and face recognition to measure the local contrast between pixels. Now a days it is also used to ensure the authenticity of digital image as it provide a comparatively robust watermark embedding technique for digital images. The main concept of LBP can be explained as:

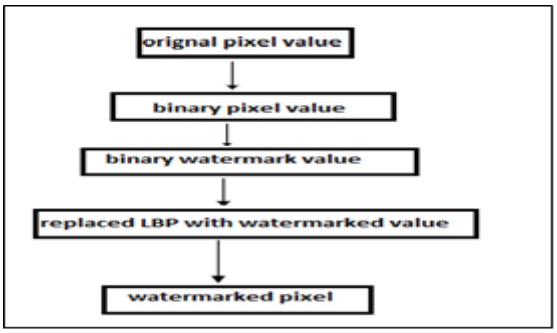


Fig 4: the process of watermark pixel value generation

Concept

In LBP technique, LBP operator is defined as, a local neighborhood surrounding a center pixel which is used as the threshold to define the local contrast of the surrounding pixels with respect to the center pixel. The surrounding pixels are labeled as 1 when the value of that pixel is greater than the center, or labeled as 0 when the value is smaller than the center. To obtain LBP code of the center pixel threshold values of neighboring pixels are multiplied with their corresponding weights and summing up them the watermark value is generated.

Watermark Embedding

In this method, three vectors are created namely gp , mp and sp. The first vector gp is used to hold the grey level values of pixels, second vector mp is used to hold the values of difference between each surrounding pixel and the center pixel, third vector sp is used to hold the binary information about each pixel based on the obtained difference between center pixel and each surrounding pixel as 1 or 0 by comparing it with the value of center pixel.

In order to embed watermark, the XOR function is used to calculate the XOR value of the whole sp vector because it has associative and commutative properties that is any circular shift of bits does not change the value of the function.

One bit of the watermark is embedded in a local region. In order to embed the watermark bit in the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

local region, the watermark bit and the XOR value of the region is compared if they are not same then only that bit is embedded in that local region. In this method author uses a 3*3 window to define local region. After successfully selecting the local region, the pixel whose value in the mp vector is minimum which is used to embed the watermark bit. If all the values of a local region are 0 or 1 then the value of the center pixel is modified in order to embed the watermark bit.

Watermark Extraction

To extract the watermark from the image simply XOR the value of each local region. It is judged accordingly, if the value is 0 the corresponding watermark bit is 0 or if the value is 1 the corresponding watermark bit is 1.

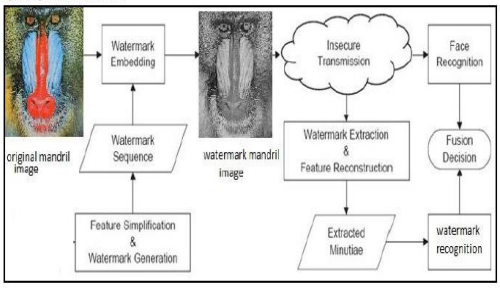
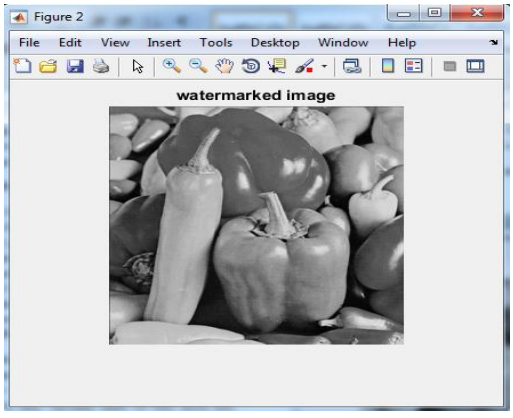


Fig 5: watermark embedding and extraction process

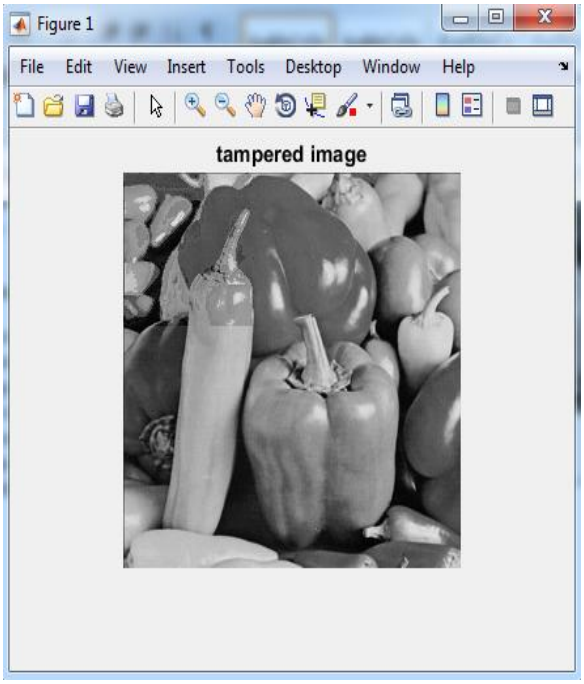
So the watermark embedding and the extraction phases are very simple but are robust against the post processing attacks like noise addition.

VII. Results and Discussions



PSNR of watermarked image 43.5431

Total number of watermarked pixels are 49964



PSNR of tampered image 30.4858

Number of pixels tampered	1 pixel	10 pixels	100 Pixels	Half pixels	All pixels	Random pixel(110,112)
PSNR of watermarked image (in db)	40.259	40.259	40.259	40.259	40.259	40.259
PSNR of tampered image (in db)	40.259	40.259	40.259	27.5538	21.3387	40.259
PSNR of recovered image (in db)	40.259	43.3558	43.1636	34.0235	28.8556	40.259
Number of watermarked pixels	49981	49981	49981	49981	49981	49981
Number of tampered blocks	0	2	12	1319	5373	0
Time taken for embedding(in seconds)	10.5712	10.5712	10.5712	10.5712	10.5712	10.5712
Time taken for detection(in seconds)	20.4918	22.8377	17.8874	18.4676	21.2188	19.5736
Time taken for Recovery(in seconds)	3.732e-006	7.464e-006	3.732e-006	8.8635e-006	9.33e-006	6.531e-006

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

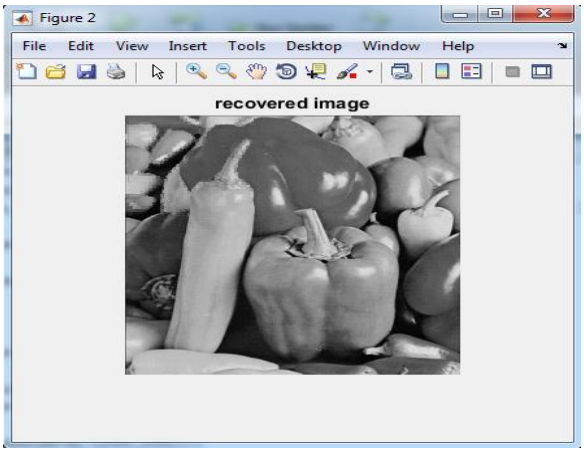


Image tampered by intruders

Number of tampered blocks are 765
Number of tamper detected blocks are 765
PSNR of recovered image 35.1879

VIII. Conclusion

Fragile watermarking is the embedding of a signal (the watermark) into an image so that modifications to the resulting marked image can be detected with high probability. A fragile marking system is useful in a variety of image authentication applications. Image authentication is a problem that can be efficiently solved with either fragile or semi-fragile watermarks.

There are many open research problems that need to be addressed in fragile watermarking system such as the development of techniques that allow the detection of authenticity without permitting mark embedding. Early fragile watermarking systems embedded the mark directly in the spatial domain of an image. These techniques embed the mark in the least significant bit plane for perceptual transparency. Their significant disadvantages include the ease of bypassing the security they provide and the inability to lossy compress the image without damaging the mark. Many important applications can benefit from the use of fragile techniques.

In this work we discussed the fragile watermarking scheme for image tamper detection and recovery. Our work is based on the concept of Local Binary Pattern (LBP).The LBP is showing the neighbourhood information of block. We observed that LBP based fragile watermarking scheme is having good result for image tamper detection and recovery. If the pixel information of image is changed or altered it will affect the LBP of that particular block and it varies with the original LBP of the block. Therefore, this modified scheme uses LBP as authentication data for self-embedding. As the authentication information is embedded into the 2 LSB of the pixel of each image block the image quality of watermarked image remains satisfactory. The various features of LBP can be used to generate watermark. LBP can be used with different radius and different sampling points in future work.

References

[1] T. Minamoto and R. Ohura, "A blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic," Sci. Direct Journal of Applied Mathematics and Computation, pp-306-319, 2014.

[2] Chandra M. B. and Srinivas K. S., "Robust multiple image watermarking scheme using Discrete Cosine Transform with multiple descriptions," International Journal of Computer Theory and Engineering, vol. 1, pp. 1793–8201, 2009.

[3] B.L. Gunjal and R.R. Manthalkar, "Discrete Wavelet Transform based strongly robust watermarking scheme for information hiding in digital images," Third Int. Conf. Emerging Trends in Engineering and Technology. India, pp. 124-129, Nov 2010.

[4] R.-J. Chen and J.-L. Lai, ''Image security system using recursive cellular automata substitution,'' Pattern Recognition, vol. 40, no. 5, 2007, pp. 1621-1631.

[5] X. Wu, Z.-H. Guan and Z. Wu, "A chaos based robust spatial domain watermarking algorithm", Advances in Neural Networks – ISNN 2007, vol. 4492, pp. 113-119, 2007.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[6] S. Rawat, B. Raman. "A chaotic system based fragile watermarking scheme for image tamper detection", Sci. Direct International Journal of Electronics and Communication, vol. 65, pp. 840-847, 2011.

[7] S.-H. Liu, H.-X. Yao, W. and Y.-L. Liu, "An image fragile watermark scheme based on chaotic image pattern and pixel pattern", Applied Mathematics and Computation, vol. 185, pp. 869–882, 2007.

[8] Z. Wenyin and F. Shih, "Semi fragile spatial watermarking based on local binary pattern operators", Optics Communications, vol. 284, pp. 3904–3912, 2011.

[9] Z. Dawei, C. Guanrong and L. Wenbo, "A chaos based robust wavelet domain watermarking algorithm", Chaos, Solutions & Fractals, vol. 22, pp. 47–54, 2004.

[10] G. Z. Yantao, M. Yunfei and L. Zhiquan, "A robust chaos based DCT domain watermarking algorithm", International Conference on Computer Science and Software Engineering, vol. 3, pp. 935 - 938, 2008.

Author Details

K. V Pratyush pursued his B.Tech in the department of Computer Science and Engineering, Gitam University, Visakhapatnam, A.P.