iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** X **Month of publication:** October 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

An Improved Secure Semi-fragile Watermarking based on LBP and Fuzzy Histogram Equalization

Rhema Singh[1], Dr. N. K Gupta[2]
[1, 2]*Department Of CSE, Sam Higginbottom University of Agriculture, Technology and Sciences, Allahabad*

Abstract: ***In this paper, we analyze a recently proposed semi-fragile watermarking scheme based on local binary pattern (LBP) operators, and note that it has a fundamental flaw in the design. . In watermark embedding process, the central pixel value of each block is taken into account and Arnold transform is adopted twice in embedding and extraction. But Arnold Transform is time consuming as it is an iterative process and require much time to perform in the embedding and extraction. The other flaw is lower Peak Signal-to-Noise Ratio(PSNR).To illustrate its weakness, two special copy-paste attacks are proposed in this paper, and several experiments are conducted to prove the effectiveness of these attacks. To solve these problems, an improved semi-fragile watermarking based on LBP operators is presented. In watermark embedding process, the central pixel value of each block is taken into account and during extraction Fuzzy Histogram Equalization is applied. Experimental results show that the improved watermarking scheme can overcome the above defects and locate the tampered region effectively with better PSNR value.***

Keywords: Semi-fragile Watermarking, Local Binary Pattern (LBP), Peak-to-Signal Ratio(PSNR),Fuzzy Enhancement, Histogram Equalization

I. INTRODUCTION

With the across the board use of advanced innovation, computerized media (especially advanced pictures) has come to assume a huge part in everyday lives. Be that as it may, the expanding utilization of picture and video altering instruments achieves a genuine danger. Copyrights and the substance of advanced media are as a rule seriously wrecked. As a compelling method for tending to this issue, advanced watermarking plan has risen at a memorable minute[1].The purpose of digital picture watermarking is to conceal some recordswithin a photograph to prove its possession or to authenticate it. Digital Watermark is the signal that is embedded into some digital media to shield their copyrights or to authenticate them. The image in which watermark is inserted is recognized as the host image. After embedding digital watermark signal in the host image, it becomes watermarked image. The use of digital picture watermarking is increasing hastily for the reason that 1990's to guard the copyrights on the digital media like audio, video and pictures or to authenticate them. Watermarking techniques developed previously were based on embedding watermark in spatial domain and allowed watermark to be visible to the observer. As compared to the formerly developed watermarking techniques, present day watermarking strategies embed watermark in a way that there is no degradation in the best of the watermarked image, as imperceptibility is one of the most important requirement of a novel watermarking technique[2]. It is safe to general picture preparing activities and delicate to noxious assaults. In this paper, assaults are exhibited to show that this watermarking plan is less secure and can't be utilized for possession insurance and alter identification. To address this issue, a protected semi-delicate watermarking calculation is displayed. Another reference esteem is ascertained by consolidating the LBP grouping and focal pixel esteem in each square. Also, a strategy called Fuzzy Histogram Equalization is used to enhance the watermark's security.

II. RELATED WORK

By and large, advanced watermarks can be characterized into three classifications including robust watermarks, fragile watermarks, and semi-fragile watermarks [3]. As the name suggests, robust watermarks are strong against general picture preparing activities and malignant assaults. Because of this property, robust watermarks are generally utilized as a part of copyright assurance [4]. Actually, fragile watermarks are vulnerable to any change, which are commonly connected in picture content confirmation [5]. Semi-fragile watermarks misuse the upsides of the over two watermarks. It is insusceptible to general picture handling activities and touchy to vindictive assaults. Therefore, semi-fragile watermarks have received more attention from researchers.Also, spatial area and recurrence space are two inserting areas utilized as a part of watermarking plan. In spatial-space watermarking, watermark message is embedded into picture by modifying the pixel esteems straightforwardly [6,7]. In recurrence space watermarking, watermark message is inserted by adjusting the change coefficients. The ordinarily utilized changes incorporate discrete cosine change (DCT)

[8,9], discrete Fourier change (DFT) [10], and solitary esteem decay (SVD) [11,12]. Contrasted with the last mentioned, the spatial-space watermarking is more defenseless to picture alterations, which is for the most part connected in delicate watermarking and semi-delicate watermarking. Over the most recent couple of years, an expansive number of semi-delicate watermarking plans have been exhibited for picture confirmation [13].

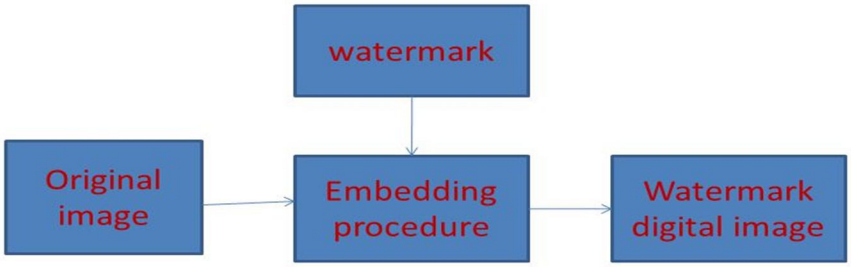


Fig2.1-Block Diagram for Watermarking Digital Image

An enhanced secure LBP-based semi-delicate watermarking is displayed in this area to take care of the issues specified above and guarantee the security of the watermarking plan. The LBP design just considers the size connection between the focal pixel esteem and neighborhood pixel esteems. The focal pixel esteem assumes a vital part as an edge. In this way, in the event that we consider the data of focal pixel esteem, it can decrease the false recognition issue to a specific degree. The watermark embedding is completed by modifying the neighborhood pixel values according to the value .To protect the watermark information, a suitable encryption method is necessary. Arnold transform is used for this purpose. After a specific no. of permutations, the changed picture can swing back to the first picture once more. So the change time k can be taken as a mystery key to encode the paired watermark picture. In the enhanced LBP-based watermarking technique, we exploit this property and perform Arnold change on watermark picture. After opposite change, the watermark will be recouped from scrambled watermark. Furthermore, it is troublesome for assailants to get the privilege watermark without redress key, despite the fact that they have taken in the extraction rules.

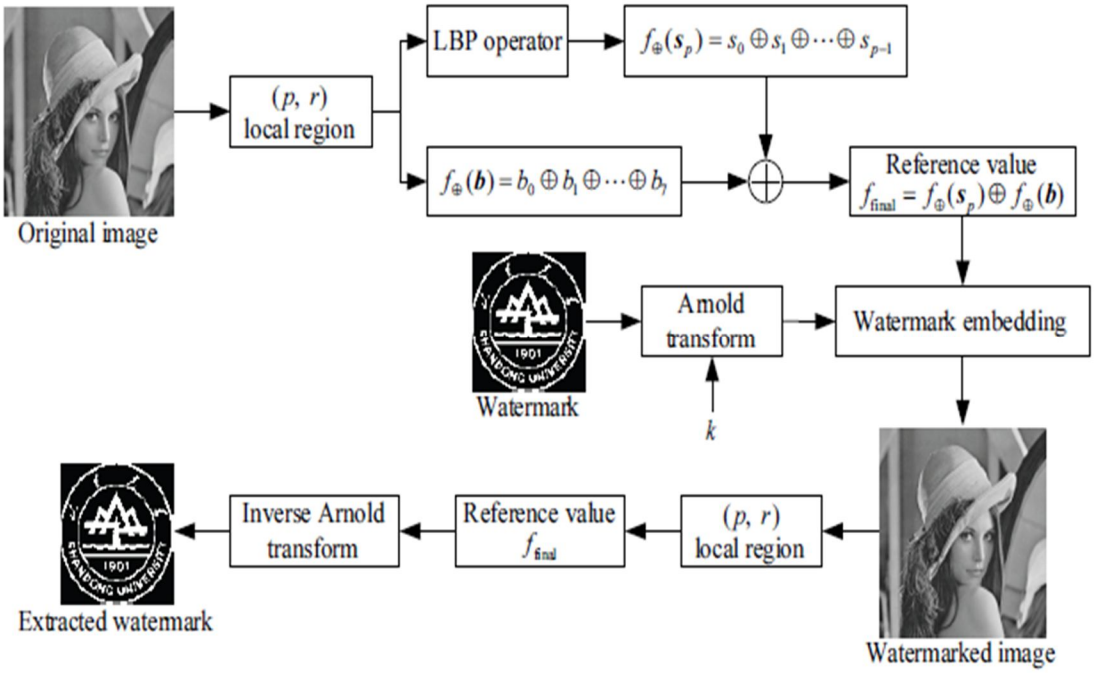


Fig2.2-Block diagram of earlier watermarking

A few investigations are directed to demonstrate the legitimacy of the recommended watermarking plan under general assaults and the proposed assaults. The Peak Signal-to-Noise Ratio (PSNR) and NC esteem are two assessment files utilized as a part of the tests.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

III. METHODOLOGY

The proposed method uses Local Binary Pattern (LBP) and Fuzzy Histogram Equalization for improving the Peak Signal-to-Noise Ratio (PSNR) value. This semi-fragile watermarking scheme uses LBP before watermarking the image and embed it with the watermark. Then in the extraction process it uses the fuzzy histogram equalization to improve the quality of the extracted watermark. It uses 2 techniques:

A. Local Binary Pattern (LBP)

The LBP administrator is a basic surface descriptor that was first proposed by Ojala et al. It mirrors the nearby differentiation between focal pixel esteem and its neighborhood pixel esteems, and this spatial relationship is at long last portrayed in a double example. With constant changes to the LBP calculation, numerous enhanced LBP administrators have been proposed, for example, uniform LBP and pivot invariant LBP. The meaning of LBP administrator depends on a circularly symmetric model. Given a span r, a circularly symmetric neighborhood p can be dictated by:

$$p = (2r + 1) - 1 \quad (1)$$

For a local region (p, r), the LBP pattern of central pixel is defined as:

(2)

$$LBP(x_c, y_c) = \sum_{i=0}^{p-1} 2^i \times S(g_i - g_c),$$

wheregc is the pixel value in central pixel (x_c , y_c) and g_i (i= 0,1,…..p- 1) refers to the pixel value inthe neighborhood. $S(x)$ is a sign function given as:

$$S(x) = \begin{cases} 1, & x \geq 0, \\ 0, & \text{otherwise.} \end{cases} \quad (3)$$

Because of its property of texture description, the LBP pattern has been broadly utilized as a part of face detection and tamper detection. In the creators brought LBP operator into watermarking plan. From that point forward, numerous LBP-based digital watermarking algorithm have been advanced. To better comprehend the LBP design and uncover the mistakes in, Fig. 1 demonstrates the first LBP administrator utilized as a part of, where r = 1 and p =8 [14].

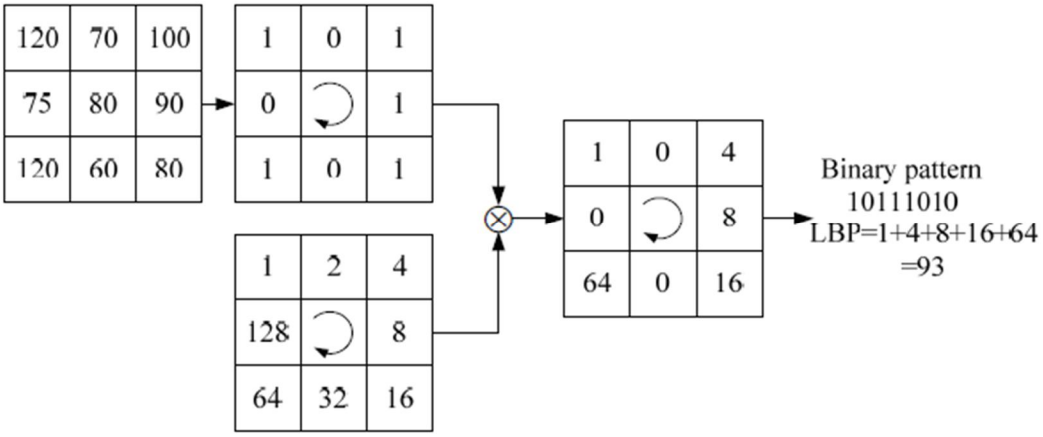


Fig 3.1- Original LBP operator used in semi-fragile watermarking

B. Fuzzy Histogram Equalization (FHE)

Fuzzy logic-based histogram equalization (FHE) is proposed for image contrast enhancement. The FHE comprises of two phases. To start with, fluffy histogram is processed in light of fluffy set hypothesis to deal with the vagary of dim level qualities bitterly contrasted with traditional fresh histograms. In the second stage, the fluffy histogram is separated into two subhistograms in light of the middle estimation of the first picture and after that evens out them freely to save picture brilliance.The block diagram for the embedding procedure is shown in Figure 4.The image used is grayscale image and the watermark image used is also a grayscale image of the size.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

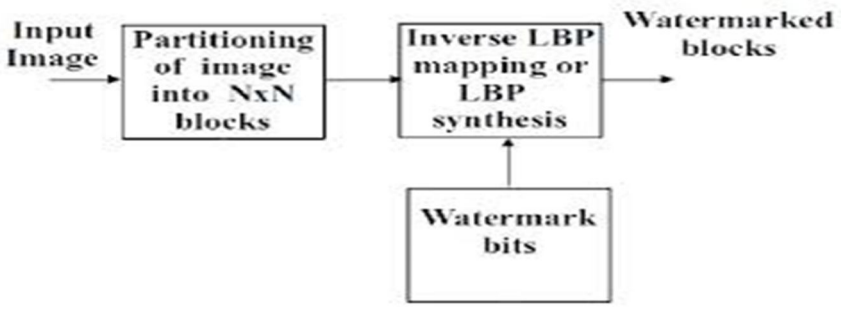


Fig 3.2-Watermark Embedding Process

The block diagram of the extraction procedure is shown in figure 5. For extraction we use the fuzzy histogram equalization to enhance the quality of the extracted watermark.

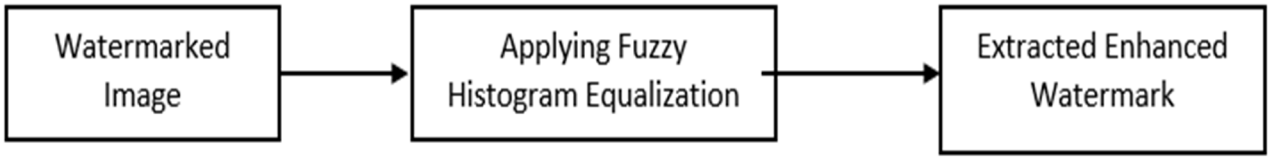


Fig 3.3- Watermark Extraction Process

1) Algorithm

a) Step 1: Input cover image.

b) Step 2: Input Logo Image

c) Step 3: Convert the cover into many (p, r) local region blocks.

d) Step 4: Calculate the difference between the central pixel value g_c and neighborhood pixel values g_i (i=0,1,…….p-1) in the (p, r) local region, and denote them as $m_p = \{m_0, m_1……... m_{p-1}\}$. Perform LBP operator on each block, and then a binary sequence $s_p= \{s_0,s_1,s_2……... s_{p-1}\}$ is generated.

e) Step 5: Compute the value of $f_{\oplus}(s_p)$ by XOR operation, which can be expressed as:

$$f_{\oplus}(s_p) = s_1 \oplus s_2 \oplus \ldots\ldots\ldots\ldots\ldots\ldots \oplus s_{p-1}$$

f) Step 6: For each image block, if the value of $f_{\oplus}s_p$ is equal to watermark bit w, the neighborhood pixel values remain unchanged; if the value is different from watermark bit w, one of the neighborhood pixel values is modified to make $f_{\oplus}s_p$ consistent with w. This process can be derived as:

$$\text{If}(w=1 \& f_{\oplus}s_p=0) \text{ or } (w=0 \& f_{\oplus}s_p=1)$$
$$\text{Then } \{\text{select } m_i = \min(m_p)\}$$
$$\text{If } (s_i=1) \text{ then } g_i = (g_i - m_i) x (1-\beta)$$
$$\text{Else then } g_i = (g_i+m_i) x (1+\beta)$$

where β represents the watermarking intensity factor. On the receiving end, the watermark is extracted from watermarked image by judging the value of $f_{\oplus}s_p$, which can be defined as:

$$\text{If } f_{\oplus}s_{p=1} \text{ then } w=1;$$

else w=0

g) Step 7: Apply Fuzzy Histogram Equalization function to enhance the extracted logo image.

h) Step 8: Calculate the performance parameters in terms of PSNR and NC.

IV. EXPERIMENTS AND RESULTS

Broad analyses have been performed on various pictures to dissect the working of the calculation. A few standard test pictures, for example, Airplane, Baboon, Lena, Barbara and so on are alluded to in the present research work for watermark installing and watermark identification. The procedure isn't constrained to the utilization these cover pictures however we have utilized them as they are standard pictures generally utilized by different scientists chipping away at picture watermarking research region.Here we are working on an image of the size of 256*256.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

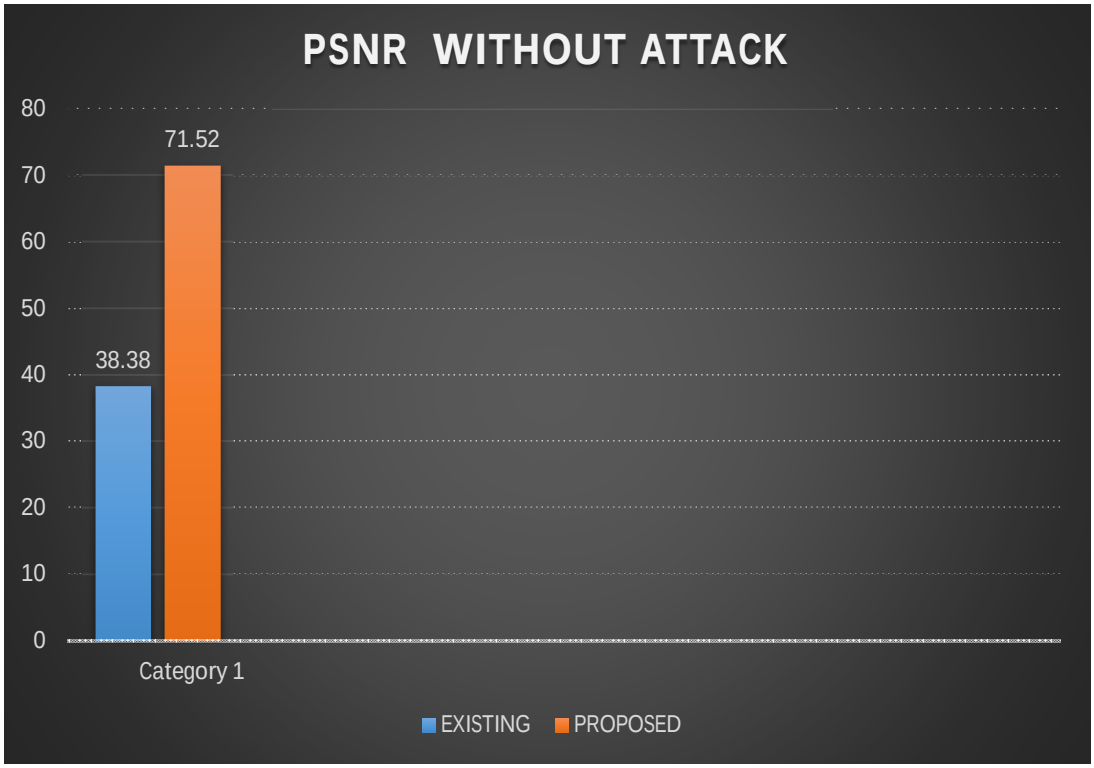


Fig 4.1- PSNR comparison between existing and proposed

This is the graph of PSNR of the existing and proposed of image watermarking showing the comparison of existing and proposed work.

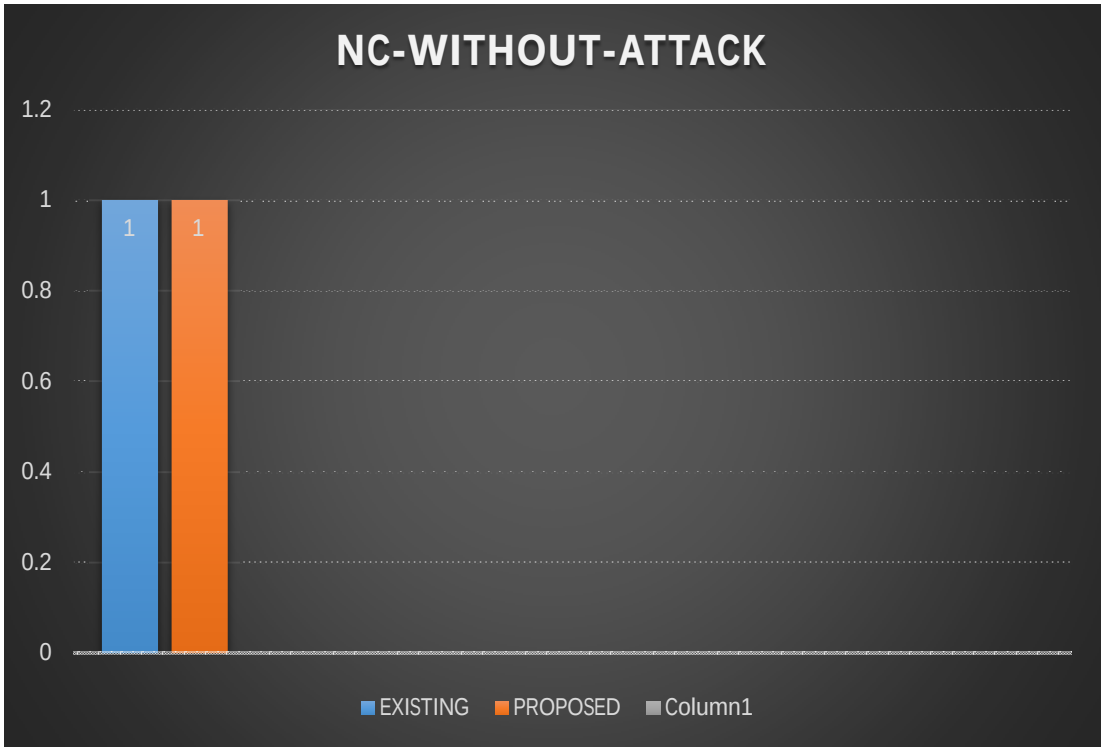


Fig 4.2-Without attack NC is same as in existing.

This is the graph of NC-WITHOUT ATTACK of the existing and proposed of image watermarking showing the comparison of existing and proposed work.

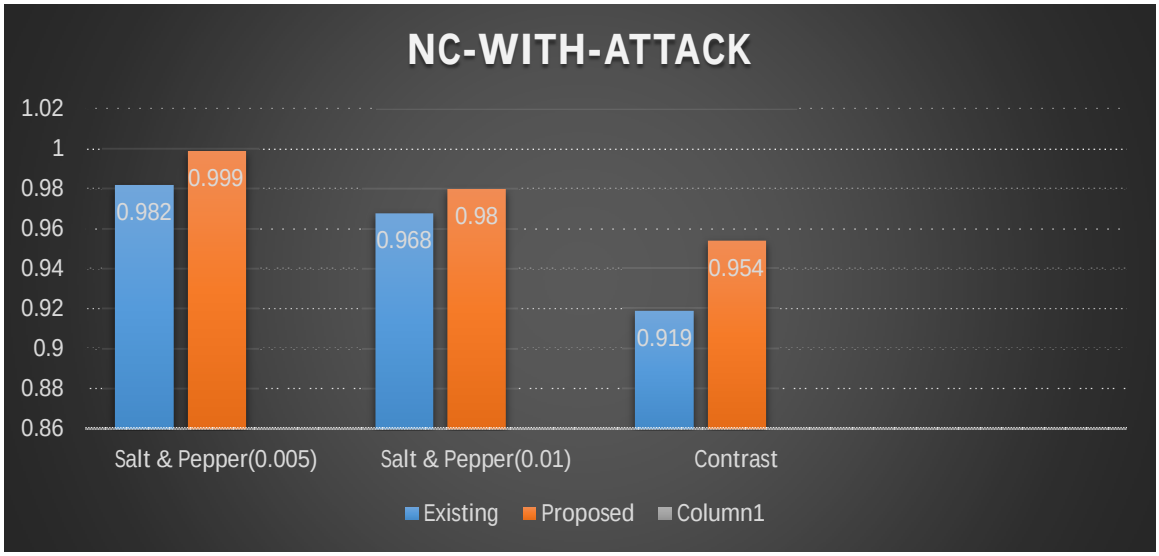


Fig4.3-Comparison between the existing and proposed NC value under different Attacks

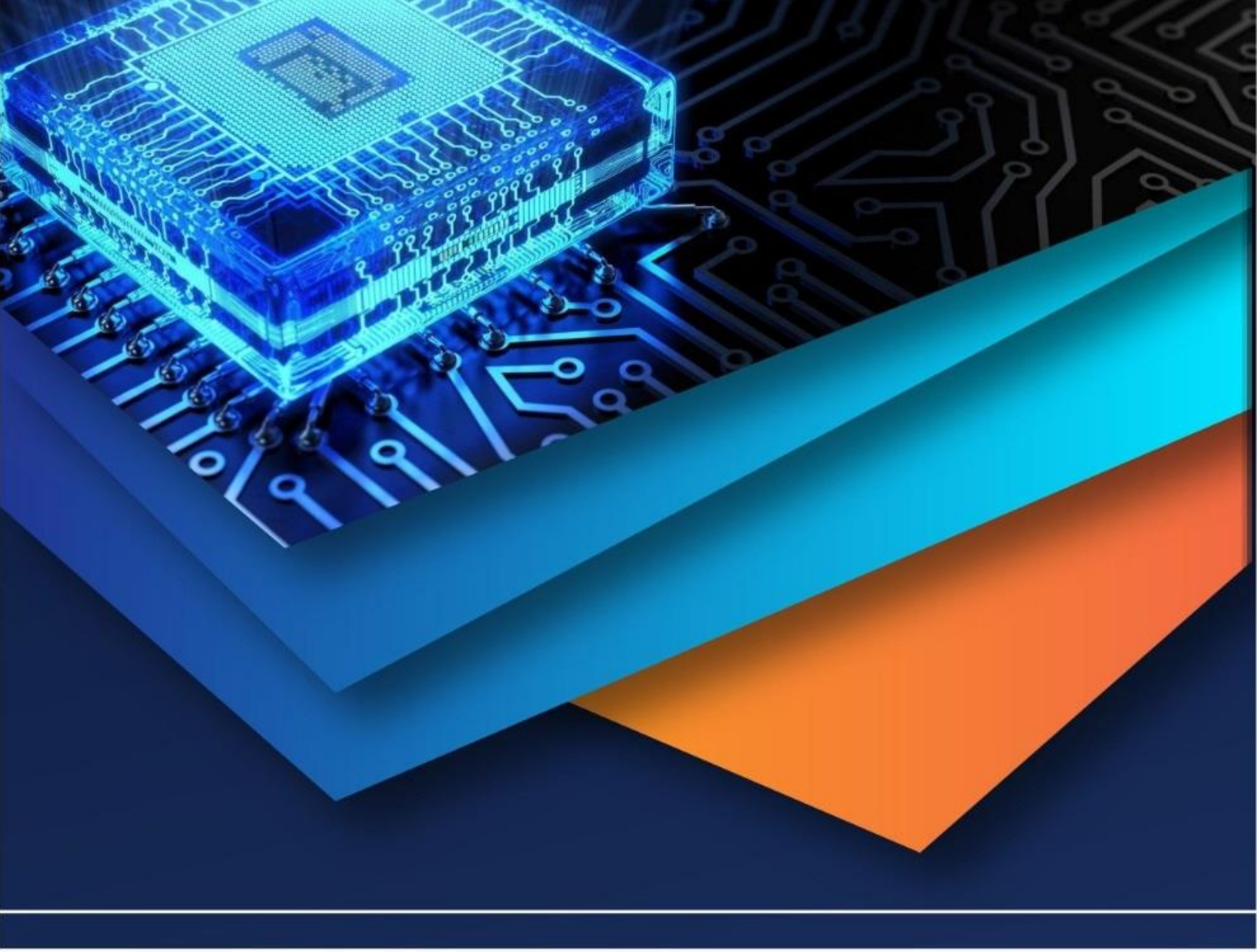
This is the graph of NC-WITH ATTACK of the existing and proposed of image watermarking showing the comparison of existing and proposed work.

V. RESULTS AND CONCLUSION

In this result paper of watermarking techniques is describe as a new development in the digital image watermarking for 256×256 in which the watermarking techniques is analysed with the help algorithm LBP (local binary operate) and FHE (Fuzzy Histogram Equalization) and it will be better than existing systemIn this paper we increase the PSNR and NC based on LBP and Fuzzy Histogram Equalization and various graph can be obtain in MATLAB tool. In the future,although the method for image enhancement based on fuzzy logic is sufficient but in future efficient methods can be develop for image enhancement which can give more accurate resultby trying to improve the PSNR and making the NC value further improved.

REFERENCES

[1] Verma and M. J. Singh, “Digital image watermarking techniques: A comparative study,” International Journal of Advances in Electrical and Electronics Engineering, vol. 2, no. 1, pp. 173-184, 2013.
[2] http://shodhganga.inflibnet.ac.in/bitstream/10603/20504/18/18_summary.pdf
[3] V. Verma and M. J. Singh, “Digital image watermarking techniques: A comparative study,” International Journal of Advances in Electrical and Electronics Engineering, vol. 2, no. 1, pp. 173-184, 2013
[4] T. Hai, C. M. Li, J. M. Zain, and A. N. Abdalla, “Robust image watermarking theories and techniques: A review,” Journal of Applied Research and Technology, vol. 12, no. 1, pp. 122-138, 2014.
[5] S. H. Liu, H. X. Yao, W. Gao, and Y. L. Liu, “An image fragile watermark scheme based on chaotic image pattern and pixel-pairs,” Applied Mathematics and Computation, vol. 185, no. 2, pp. 869-882, 2007.
[6] T. Y. Lee and S. D. Lin, “Dual watermark for image tamper detection and recovery,” Pattern Recognition, vol. 41, no. 11, pp. 3497-3506, 2008.
[7] S. Rawat and B. 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.
[8] S. D. Lin, S. C. Shie, and J. Y. Guo, “Improving the robustness of DCT-based image watermarking against JPEG compression,” Computer Standards &Interfaces, vol. 32, no. 1-2, pp. 54-60, 2010.
[9] Y. F. Zhu and L. Lin, “Digital image watermarking algorithm based on dual transform domain and selfrecovery,”International Journal on Smart Sensing and Intelligent Systems, vol. 8, no. 1, pp. 199-219, 2015.
[10] V. Solachidis and I. Pitas, “Circularly symmetric watermark embedding in 2-D DFT domain,” IEEE Transactions on Image Processing, vol. 10, no. 11, pp. 1741-1753, 2001.
[11] J. M. Guo and H. Prasetyo, “Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition,” AEU - International Journal of Electronics and Communications, vol. 68, no. 9, pp. 816-834, 2014.
[12] S. Dadkhah, A. A. Manaf, Y. Hori, A. E. Hassanien, and S. Sadeghi, “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.
[13] A. Tiwari and M. Sharma, “Comparative evaluation of semifragile watermarking algorithms for image authentication,” Journal of Information Security, vol. 3, no. 3, pp. 189-195, 2012.
[14] http://jips-k.org/file/down?pn=800



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY