International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

ENHANCEMENT OF IMAGE QUALITY USING EFFICIENT WATERMARKING ALGORITHM AGAINST UNAUTHORIZED ALTERATION

D.J.Pricilla Mary[1*], R.Jagadeshwaran[2*], R.Geethalakshmi[3]

[1,2,3]AP, ECE, Saveetha Engineering College

ABSTRACT

Image processing is a vital role in the field of communication to exploit the information. The information received will provide high efficiency compare all other fields of communication. Fake photography or image alteration is one of the counterfeit in the communication or in many applications. This unauthorized alteration generates a problem when the user wants to authenticate the image. This paper enhances the image against this tampering or unauthorized alteration of duplicate image and maintain the PSNR of the image. The image is compressed and watermarked or authenticated, then transmitted through the channel using hash function. Watermarking is carried at various level of bits and PSNR value is calculated using SPIHT and compared with Lempe1-Ziv-Welch (LZW). The results showed that SPIHT is better in terms of PSNR values. The copyright of the image makes it genuine and provide protection against unauthorized alteration. The receiver applies the hash function and remove the watermark to unwrap the original image. Finally, the image reconstructed using SPIHT decompression to regain the original image. The PSNR of the original image and reconstructed image is 39.564 db and 36.9 db respectively.

Keywords: PSNR, SPIHT, Tampering detection, Watermarking.

I. INTRODUCTION

Digital image or photography is the most powerful technique for media expression to prove evidence in the field of forensic, scientific research, Intelligence and crime detection. Digital image is also considered as secret weapon for communication, which provides exact information to all users. Digital image processing is the enhancing field to process the image by means of acquisition, enhancement, segmentation, Extraction and Classification. Digital image processing has its root in the field of numerous applications like Textiles, Film Industry, Graphical arts, Military, Medical Imaging, Remote Sensing, signal processing [5] etc.

The field of Image processing have developed to increase the image quality by removing the noise or any kind of irregularities in the image. Noise may creep in the image during image acquisition or image transformation into the channel. The numerous algorithm had developed to reduce the various image noise. But this reduce the image quality by decreasing or increasing the pixel value. Hence original or genuine image may not be retained.

Image tampering [10] is related to the unauthorized image alteration or image damage. The authorized alteration leads to increase the image quality or changing the pixel value voluntarily. The unauthorized image alteration emerged as a photo fakery, it created a critical problem in the field of Image processing. In Early 1840, Hippolyte Bayard, was the first person to create a fake photography. From this, all the other work related to fake photography have developed.

Image tampering become the successful tool in the field of Film industry and entertainment. But, in forensic it become tedious to the judgement case. Image tampering may occur naturally due to natural disaster or in meteorological. In meteorological tampering detection done to compare the variation of cyclone position in minute difference. The tampering detection is a currently undergoing research topic evolved to create authenticity of digital photographs [1].

Watermarking [11] is the process of hiding the multimedia information for copyright marking. Watermarking embedded a legal right [14] and authentication [15] for the information to ensure the image was not altered. Hence the watermarking ensure that the image was not altered unauthorizedly. Water marking was coined in early 1990's by Andrew Tirkel. The watermarking has various application like authentication, Source tracking and trademark etc.

This paper involved in the tampering detection using efficient watermarking algorithm to reduce the unauthorized image alteration. The image integrity maintained by the watermarking algorithm and originality of the image is maintained. The parameter involved in the tampering detection are watermarked image quality, Tolerable Tampering Rate (TTR) and content recovery quality.

The paper divided into 6 sections. The section 2 deals briefly with Digital watermarking techniques. Section 3, presents the image tampering detection techniques. An efficient watermarking algorithm presented in section 4. The image tampering detection using the proposed watermarking algorithm discussed in section 5. Finally, the experimental result and its parameters are concluded in last section.

II. WATERMARKING

Watermarking is the technique to protect the information or image by hiding some other information into it which may or may not be related to the source. Watermarks are mainly used to verify or identify the owners of the image or information. Watermarks should not affect the quality of the source image [5]. if it affects, the purpose of watermarks become useless. The watermark never changes the size of the source image unlike metadata does. Watermark should be efficient enough to robust against the unauthorised alterations. Watermark will not degrade or control the access of source image. If any person makes alteration without the knowledge of the owner (i.e) attack, detection algorithm is applied to extract the watermark from it [8]. The major application of watermarks is tracking of source, Management of contents on social networks, authentication of videos. Basically, watermarking is protection tool against Tampering.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

III. TAMPERING DETECTION TECHNIQUES

Tampering is the process of unauthorized alteration of the image. The other term 'Steganography' is the process of the hiding the information for secret communication [3],[4]. Steganography has its roots dated long back. Steganography is the process of hiding the bibliography over their image. The truth behind the image hidden by the tampering and it retained by steganography. Tampered image looks as natural as possible to the viewers with some parts of the host image replaced by the different image. Figure 3.1 shows the steganography image and the message retrieved from the image. In case of tampering, data was not hidden, only the image was altered by the other image.

(a) (b) (c)

Figure 3.1 (a) Original image (b) Steganoed image (c) Retrieved image

The detection of tampering is divided into two categories such as active detection and passive detection. In active detection, watermarking of the image carried at the time of image capturing and authenticate immediately. Hence the image tampering can be greatly reduced [6]. The genuine of the image maintained. But all the image must have watermarked and transmit through the channel to the end users.

The Passive detection [13],[14] techniques neither require image watermarking process nor prior information by capturing the image. It requires the statistical properties of the original image to detect the tampering. There are two methods of passive detection: cloning and splicing detection techniques. In cloning detection, the original image is pasted on the received image and find the correlation between the image. the tampered image may be compressed or increased in resolution results in mismatch in the correlation of the image. Hence the image tampering can be detected, and that pixel value can be localized.

IV. PROPOSED WATERMARKING ALGORITHM

The image tampering detection is design and developed with Watermarking algorithm. The process is split into two stages. The first stage involves in hiding the input image with unauthorized image or data. The second process involves in detecting that unauthorized alteration using an efficient watermarking algorithm. Figure 4.1 shows the processing steps of unauthorized alteration, this may happen in image acquisition or image transfer via channel.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

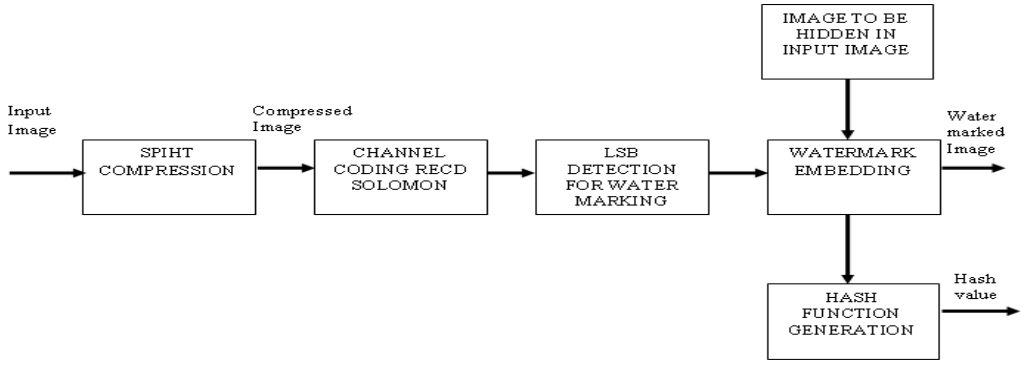

Figure 4.1 Proposed Watermarking Algorithm

4.1 Spiht Compression

Set Partitioning In Hierarchical Trees (SPIHT) is a compression technique of an image that utilize the similarities using wavelet decomposition of an image. The spectral behaviour of signal transformed from time (Spatial) domain into frequency domain using Fourier transform [7]. The non-stationary properties of the signal represented using this Fourier transform. Inorder to localize the spatial domain, window function is introduced to the signal before frequency conversion. The window size can be changed dynamically, and it detect the distinct spaces and scales of the information locally.

$$\int_{-\infty}^{\infty} \frac{|\hat{\psi}(w)|}{|w|}\, dw \;<\; \infty \text{..(1)}$$

ψ - Basic Wavelet. Equation (1) implies that $\hat{\psi}(0) = 0$,

$$\int_{-\infty}^{\infty} \psi(x)\, dx = 0 \qquad \text{..(2)}$$

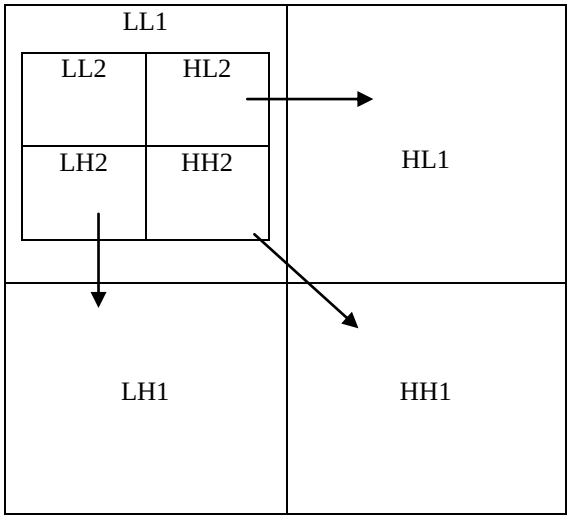

Figure 4.2 SPIHT Image compression

It provides the Highest Image Quality, Progressive image transmission, fully embedded coded file, Simple quantization algorithm, fast coding/decoding, completely adaptive, Lossless compression, Exact bit rate coding and Error protection. SPIHT makes use of four levels –LL, LH, HH, HL as shown in figure 4.2. (L represents LOW, H represents HIGH). For example, if the bit has the pixel value as 8.6 it assumes as 9 (HH) in other case if it has 8.4 means it assumes the value as 8(LL). It also reduces the memory space required to store the image. The result is in the form of a bit stream. It recovers the image perfectly by coding all bits of the transform.

4.2 Reed Solomon Code

The group of non-binary cyclic code to correct the error produced while image SPIHT compression is Reed Solomon code. This code localizes the pixel error value and correct it using erasure code. The code comprises of erasure code and error correcting pixel location. For each image code is generated and transmit to the end user. The receiver can find the image is altered with the help of this code. The code maintains the image compression ratio.

4.3 Lsb Watermarking

The watermarking of the image is the process of varying the pixel values of the pixels location's in the image. The watermarking provides trademark to the image, while maintain the image quality. In an efficient watermarking algorithm, the Least Significant Bit (LSB) is chosen for embedding watermark and the secret key is provided to the end user. The LSB change does not affect the image quality and it retains the image information. Example, if 8^{th} LSB is used for watermarking, the result obtained is better when compared to other significant bits. The 8-bit binary value is 00000100 (4), if it uses 8^{th} bit for watermark then the watermarked data will be 00000101 (5), it produces only small changes and thus gives better result.

4.4 Hash Function

Hash function map the data to fixed size instead of arbitrary size. The hash function provides high integrity and authentication for transmitted image. The hash function maintains the table; hence each hash value denotes a pixel value and transmitted through the channel. At the receiver side, the data recovered from the channel and with the help of hash code it is reconstructed to generate the original image.

V. TAMPERING DETECTION USING WATERMARKING ALGORITHM

The previous section deals with a watermarking process. This section deals with tampering detection using a watermarking algorithm. Figure 5.1 shows the tampering detection using watermarking algorithm. The tampering detection done with the Hash function generated in the watermarking process. The tampering detection process is the reverse process of the watermarking algorithm.

5.1 Tampered Detection

The received image is given as input to the hash function generation block. It generates the hash function according to the input side. By applying the hash function to the watermarked image, the copyright of the image

is authenticated and analyse the unauthorized alteration of the image. In tampering detection block, the hash values of the received image and watermarking decomposed image are compared to check whether the image is tampered. The received hash value and decomposed image hash value are different then image is tampered, if it is same then the image is not tampered. The least significant bit and secret key are selected by which the watermark embedding is performed for the image. By these parameters watermark decomposition is performed, and tampered blocks are detected. The bits which are tampered assumed to be erased. The figure 5.1 provide the steps involved in the tampering detection techniques.

5.2 Re-Constructing Original Image

The original image was received by image reconstructing [2] the tamper detected image. reconstruction of the image done with the help of Using Reed Solomon channel decoding, where the lost bits are restored by reference bits of the original image. The self-recovered image is decompressed using SPIHT decompression algorithm. Finally, the original image is reconstructed with high image quality and acceptable Peak Signal to Noise Ratio (PSNR).

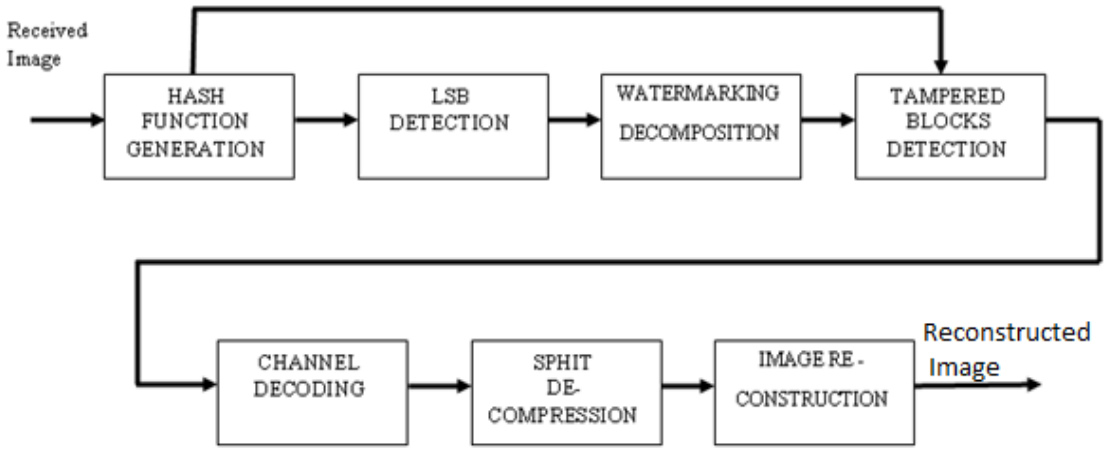

Figure 5.1 Tampering Detection using Watermarking

VI. RESULT AND DISCUSSION

In this section, we discuss the results obtained by the proposed algorithm. The results discussed for the 'Lena' image of size 512 × 512 to evaluate the unauthorized alteration. Figure 6.1 shows the image reconstruction from the unauthorized image. The host image of 512 × 512 is 6.1(a). The host image is authenticated using the watermarking algorithm. This provide the copyright to the image and ensure the genuine nature of the image. the watermarked image is shown in figure 6.1(b).

The watermarked image is like the host image, since the LSB detection method of efficient watermarking techniques is used. The image quality was not degraded at any cost. The pixels value gets reduced, this reduce

the brightness of the image while retaining the image quality. The watermarking process carried for the SPIHT compressed image. SPIHT compress the image in the ration of 4:1, that reduces the image storage and transmission bandwidth.

The watermarked image is transmitted through the channel and received at the end user. The image is unauthorized using the different image. The host image is altered and tampered. In the lena image, the information altered by adding the flower in the cap. The hash function generated in the watermarked image and hash function generated in the tamper detection technique are compared. The pixel values are different then the intensity value of '1' and if it is same then the intensity value is '0'. Hence the tampered image position is localized, and it is detected.

Finally, the image is reconstructed by SPIHT decompression technique. The SPIHT decompression enhance image in the ratio of 1:4. Hence the image is reconstructed in same process of compression. The PSNR is calculated for the image to evaluate the image quality. PSNR defined the ratio of the maximum possible power of the signal to the power of corrupting noise. PSNR affect the image fidelity. The PSNR of the received signal is calculated and found as 36.9 db and for the original image it is calculated as 39.564 respectively.

(a) (b) (c)

(d) (e)

Figure 6.1 (a) Host image (b) Watermarked lena image (c) Tampered image (d) Tampering detection (e) Re-constructed original image

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 6.2 Watermarked at various bit level (a) 7th bit (b) 6th bit (c) 5th bit (d) 4th bit (e) 3rd bit (f) 2nd bit (g) 1st bit (h) 0th bit

Watermarked Bit level	PSNR Value (db)
7th bit (MSB)	8.99
6th bit	15.07
5th bit	20.95
4th bit	26.80
3rd bit	32.19
2nd Bit	36.33
1st Bit	38.50
0th bit (LSB)	39.27

Table 6.1 PSNR value for watermarked images at various bit levels

The watermarking process is carried using LSB bit of the image after SPIHT compression. The Watermarking process comparison is done for various bit level change and the image quality is calculated. It is found that the image quality is preserved approximately when the watermarking is done for LSB bit. The image degradation is

found for the MSB bit watermarked image. The various bit comparison is done and image is shown for various bit in figure 6.2. The calculated PSNR value is shown in table 6.1. and its corresponding graph in figure 6.3.

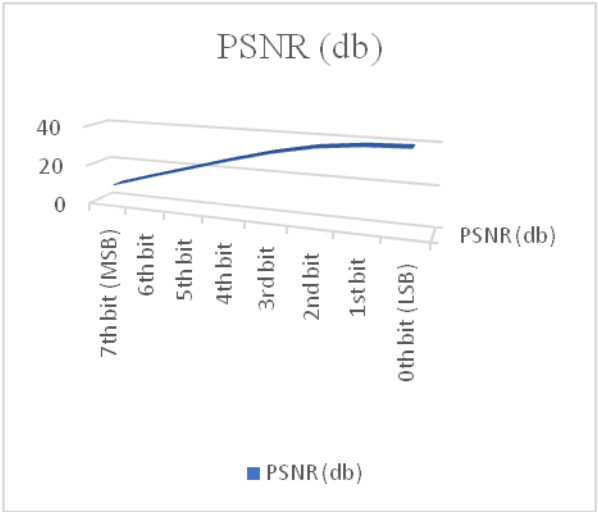

Figure 6.3 PSNR (db) vs bit level

VII. CONCLUSION

The Efficient watermarking algorithm achieved authentication against tampered image and maintaining the image quality with the efficiency of 93.2%. The watermarking of the authenticate the genuinely of the image. The proposed method provides both authentication and detection of unauthorized alteration in the image. The reconstructed image has the PSNR value of 36.9 db which is very close to the PSNR value of the original image. SPIHT compression reduce the pixel ratio and maintain the PSNR value while decompressing the image. Hash value exploit the image integrity while watermarking and reconstructing of the image. The PSNR value of original image is 39.564 db and for reconstructed image is 36.9db.

REFFERENCE

[1.] C. M. Pun, X. C. Yuan and X. L. Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, 2015, pp. 1705–1716.

[2.] Chun-shien Lu and Hong-yuan Mark Liao, "Multipurpose Watermarking for image Authentication and protection", IEEE transactions on image processing, vol. 10, n0. 10, 2001, pp.1579-1592.

[3.] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digital Investigation, Elsevier, vol. 9, issue 1, 2012, pp. 49–57.

[4.] J. Fan, T. Chen and J. Cao, "Image tampering detection using noise histogram features," Digital Signal Processing (DSP), 2015 IEEE International Conference on, Singapore, 2015pp. 1044–1048.

[5.] Jagadeshwaran R, Selvi M and SakethManukonda, "Analysis of FHSS receiver using BPSK demodulation in VHDL", Middle East Journal of Scientific Research, vol.24, 2016, pp.113-117.

[6.] M. A. Qureshi, and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," Signal Processing: Image Communication, vol. 39, part A, 2015, pp. 46–74.

[7.] MusaedAlhussein, "ImageTampering Detection Based on Local Texture Descriptor and Extreme Learning Machine", International Conference on Computer Modelling and Simulation (UKSim), 2016, pp. 196-199 .

[8.] Patrick Korus and Dziech, "A novel approach to adaptive image authentication," in Proceedings of 18th IEEE International Conference on Image Processing (ICIP),2011, pp. 2765–2768.

[9.] Patrick Korus and Dziech, "Efficient method for content reconstruction with self-embedding," IEEE Transactions on Image Processing., vol. 22, no. 3, 2013, pp. 1134–1147.

[10.] Saurabh Agarwal and Satish Chand, "Imagetampering detection using local phase based operator", International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES), 2016, pp.355 – 360.

[11.] Simon Bravo-Solorio, C.-T. Li, and Nandi A.K, "Watermarking method with exact self-propagating restoration capabilities," in Proceedings of IEEE International Workshop on Information Forensics Security (WIFS), 2012, pp. 217–222.

[12.] Xinpeng Zhang, Shuozhong Wang, Zhenxing Qian, and Guorui Feng, "Reference sharing mechanism for watermark self-embedding," IEEE Transactions on Image Processing, vol. 20, no. 2, 2011, pp. 485–495.

[13.] Xinpeng Zhang, Zhenxing Qian, Yanli Ren, and Guorui Feng, "Watermarking with flexible self-recovery quality based on compressive sensing and Compositive reconstruction," IEEE Transactions on Information Forensics Security, vol. 6, no. 4, 2011, pp. 1223–1232.

[14.] Zhenxing Qian, Guorui Feng, Xinpeng Zhang, and Shuozhong Wang, "Image self-embedding with high quality restoration capability," IEEE Transactions onDigital Signal Processing, vol. 21, no. 2, 2011, pp. 278–286.

[15.] Zhenxing Qian and Guorui Feng, "Inpainting assisted self-recovery with decreased embedding data," in proceedings of IEEE International Conference on Signal Processing, vol. 17, no. 11, 2010, pp. 929–932.