IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DIGITAL IMAGE PROTECTION AND SELF-RECOVERY USING WATERMARK ALGORITHM

Kripa Biju*, Rekha K.S
* M.tech Student, Dept. of Computer Science, College of Engineering, Kidangoor, India
Assistant Professor, Dept. of Computer Science, College of Engineering, Kidangoor, India

DOI: 10.5281/zenodo.571749

ABSTRACT

Expansion of the Internet has increased the availability of digital data such as audio, images and videos to the public. Watermarking is a method for inserting the watermark information into an image, which is to be later used for inventing tampered region and recovering the lost data in the tampered zone. The main reason for developing digital watermarking research is to protect intellectual properties of the digital world. Watermarking techniques may divide on the basis of domain like spatial domain or transform domain or on the basis of wavelets. The spatial domain techniques work on the pixels and the frequency domain works on the transform coefficients of the image.

KEYWORDS: Watermarking, Spatial domain, Frequency domain, Huffman, PN sequence, SPIHT, Reed-Solomon, Permutation, Hash detection.

INTRODUCTION

Watermarking (data hiding) [1]-[3] is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. Digital watermarking has attracted considerable attention and has numerous applications, including copyright protection, authentication, secret communication, and measurement [4], [5]. Whether watermarking algorithm is valid or not, is mainly based on two following characteristics: First, the invisibility, which means that watermarking should be invisible and do not affect original digit to be protected; Second, the Robustness, which means that extracted watermarks are still significant after suffering from all kinds of signal processing such as filtering, compressing, rotating, scaling, cropping operations, etc. [6] Now, all watermarking algorithms, according to its embedded way on the whole, can be classed into two types: the space domain and the transformation domain. They have different characteristics, from the point of view of the ability to resist attacks. Transformation domain algorithms are widely thought better than those of the space domain.

Initially, watermarking method obtains a checksum of the image data and then embeds the checksum into the LSB of randomly chosen pixels. Others add a modified maxima length linear shift register sequence to the pixel data which can identify the watermark by using spatial cross correlation function of the modified sequence and part of the watermarked image. Watermarks can modify the images spectral by modulating DCT, DFT or DWT coefficients according to a sequence known only to the owner. As a result, the security level of the watermark in the image increases while maintaining the imperceptibility of the mark.

LITERATURE SURVEY

In case of images, watermarking techniques are classified based on two working domains. Spatial Domain in which Pixels of one or two randomly selected subsets of an image are modified based on perceptual analysis of the original image and Frequency Domain in which values of certain frequencies change.

Spatial domain based techniques:

Watermarking method based on the spatial domain scatters information to be embedded to make the information more secure so that it is very difficult to detect. It uses minor change of the value of pixels. This approach has an advantage which is it is strong for cropping and translation. Various approaches for spatial domain techniques have been proposed so far which are checksum techniques, two dimensional spatial watermark, spread spectrum approach are some of them.

LSB technique

In this approach [7], LSB hides data in the spatial domain. The image is as a matrix NxM where N and M are the dimensions of the image and the value of the pixel in the position (i, j) is a binary number. This binary number can be then divided into a most significant bit (MSB) which contains a lot of information and a least significant bit (LSB) which contains very few information .Changes to the value of the LSB without distortion for the image.

Limitations of Spatial domain techniques such as LSB are easier to implement, but they are limited in robustness, which is not expected in any watermarking applications. It can survive simple operation such as cropping, any addition of noise. However lossy compression is going to defeat the watermark. An even better attack is to set all the LSB bits to 1 fully defeating the watermark at the cost of negligible perceptual impact on the cover object.

Checksum technique

In this approach [8], watermark is formed from the checksum value of the seven most significant bits of all Pixels. A checksum is the modulo-2 addition of a sequence of fixed-length binary words which is a type of hash function. This technique randomly chooses the locations of the pixels that are to contain one bit of the checksum. The pixel locations of the checksum together with the checksum value form the watermark which must be kept secret. To verify the watermark, the checksum of a test image is obtained and compared to the watermark. Advantages of this technique are mentioned below: Embedding watermark only changes half of the pixels that covered by it, as a result it not only reduces visual distortion but also increases security. An image may hold many watermark as long as they do not overlap

Limitation of this technique is any change to either the image data or the embedded checksum can cause the verification procedure to fail.

Basic M-sequence approach

In this approach [9], watermark is formed based on using a modified m-sequence. A linear feedback shift register with n stages can form pseudo-random binary sequences with maximum period of 2n-1. Two types of sequences may be formed from an m-sequence: unipolar and bipolar. Advantages of this technique are mentioned below: Watermark is robust to small amounts of noise, in the image. Successive watermarks treat the previously watermarked image as a new. An attacker can deduce watermark if 2n consecutive bits in it are known.

Limitation of this method is that it does not protect the DC value of the pixels covered by an individual block.

Secure Spread Spectrum Watermarking for Multimedia:

This approach [10], inserts a watermark into the spectral Components of the data using the techniques which are Analogous to spread spectrum communication, therefore hiding a narrow band signal in a wideband channel Advantages of this technique are mentioned below: The watermark is difficult to remove for an attacker even when several individuals combine together with independently watermarked copies of the data. It is robust to common signal and geometric distortions such as digital-to-analog and analog-to-digital conversion, re-sampling, and requantization including dithering and recompression and rotation, translation, cropping and scaling.

Frequency domain based techniques.

Transform coefficients are modified instead of directly changing the pixel values. To detect watermark, the inverse transform is used. The transforms commonly used for watermarking purposes [11],[12] are the discrete cosine transforms (DCT), discrete Fourier transforms (DFT) and discrete wavelet transforms (DWT).

Discrete Cosine Transform (DCT)

To embed a watermark, a frequency transformation is applied to the host data. Then, modification are made to the transform coefficients. DCT represents data in terms of frequency space rather than an amplitude space. This is helpful because that corresponds more to the way persons identify light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are not easy to implement and are computationally more costly.

Discrete Fourier Transform (DFT)

DFT has invariance to translation, rotation, scaling, the DFT-based Digital Watermarking Algorithm has unique advantages in the resistance geometric transformations. At present, the research of Image watermarking techniques require a relatively higher robust of watermark, an algorithm with pseudo-random noise to construct the watermark and use test to find the watermark in detected. When the image be detected extracted test sequence has a strong relevance with the original watermark. Basically the Fourier transform is a most popular technique for signal analysis, signal study and synthesis to define the effect of various factors on signal. Sometime the Fourier transform is use to transform the signal from time domain to frequency domain or signal from frequency domain to time domain. This transformation is reversible and that maintaining the same energy.

Discrete Wavelet Transform (DWT)

Wavelet domain is a secure domain for watermark embedding. Wavelet has reference to tiny waves. Discrete Wavelet Transform is based on tiny waves of limited period and unstable frequency. This is a frequency domain technique in which firstly original image is transformed into frequency domain and then its frequency coefficients are modified in accordance with the transformed coefficients of the watermark and watermarked image is obtained which is very much robust. DWT decomposes image hierarchically, providing both frequency and spatial description of the image. It decompose an image in mainly three spatial directions i.e., horizontal, diagonal and vertical in result separating the image into four different components that is Low_Low, High_Low, Low_High and High_High.

For second level of decomposition any one sub-band is chosen and is further decomposed into four levels. Maximum the level of decomposition, maximum will be the strength of the watermarked image. At every level of decomposition, the magnitude of DWT coefficients is bigger in lower bands (Low_Low), and is smaller in other three bands (Low_High, High_Low, and High_High). Larger magnitude of wavelet coefficients shows their higher significance in comparison with the wavelet coefficients of smaller magnitude. Human Visual System is extra sensitive to the low frequency parts (the Low_Low sub-band), so watermark is first located in other three sub-bands to maintain the quality of original image.

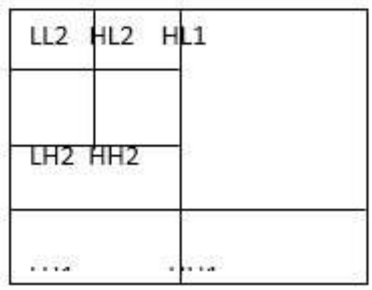

Fig.1.two-level DWT decomposition

Image tampering and protection using watermark algorithm:

Tamper Detection

Digital images not only provide forged information but also work as agents of secret communication. Users and editing specialists manipulate digital images with varied goals. Scientists and researchers manipulate images for their work to get published; medical images are tampered to misrepresent the patients‟ diagnostics, photo and yellow journalists use the trick for creating and giving dramatic effect to their stories, politicians, lawyers, forensic investigators use tampered images to direct the opinion of people, court or law to their favour and so on. Hence, distinguishing the original images from faked lots and establishing the authenticity of digital photographs have become some of the greatest challenges of the present time. Retouching, splicing, copy-pasting, cropping, cloning etc are some of the popular techniques used for image manipulations. In additions to these techniques there also exists a wide range of Steganographic methods those use this popular digital media for secret data transmission.

Tamper Detection Techniques

Digital image tamper detection techniques can be broadly classified into two groups such as active detection techniques and passive (blind) techniques. The active techniques require a pre-processing step and suggest embedding of watermarks or digital signatures to images so as to authenticate them. The major difficulty with this technique is that it requires the watermark to be embedded at the time of image capturing and for this; all digital cameras should have a standard inbuilt watermark. On the other hand, the passive detection techniques do not require pre embedding of any watermark or digital signatures to the images and hence are commonly used for the purpose of tamper detection in digital images.

Active Methods of Tamper Detection

Active tamper detection techniques [13] due to their inherent limitation, though, are not as common as those of the passive techniques still these are considered to be most efficient image authentication methods and a lot of research has been done in this field. These active image authentication techniques are commonly classified into two categories: the first method uses a fragile watermark, which localizes and detects the modifications to the contents. While the rate of tamper detection is very high for these methods they cannot distinguish between the simple brightness, contrast adjustments and replacement or addition of scene elements. Increasing the gray scales of all pixels by one would show a big area of tampering by this method, even though the image content remains unchanged for all practical purposes. The second method uses a semi-fragile watermarking, that only detects the significant changes in the image while permitting content-preserving processing. The fragile watermark though has fine localization and protection properties but cannot differentiate forgeries such as addition or removal of parts of image, from the innocent image processing operations such as brightness or contrast adjustments. solves this problem through new hybrid image authentication watermarking scheme that combines both the fragile and a robust watermark. The hybrid watermark can be used to exactly locate alteration with distinguish forgeries from other innocent operations.

Passive Methods of Tamper Detection

The passive methods are regarded as evolutionary developments in the area of tamper detection. In contrast to the active authentication techniques these methods neither require any prior information about the image nor necessitate the pre embedding of any watermark or digital signature into the image. The underlying assumption that is the basis of these schemes is, though the carefully performed digital forgeries do not leave any visual clue of alteration, they are bound to alter the statistical properties of the image. The passive techniques try to detect digital tampering in the absence the original photograph as well as without any pre inserted watermark just by studying the statistical variations of the images [14]. Researchers of passive detection techniques generally focus on two types of passive methods, the copy-move forgery detection or cloning and splicing.

Cloning Detection

To clone or copy and paste a part of the image to conceal an object or person is one of the most commonly used image manipulation techniques. When it is done with care, it becomes almost impossible to detect the clone visually and since the cloned region can be of any shape and size and can be located anywhere in the image, it is not computationally possible to make an exhaustive search of all sizes to all possible image locations. According to any Copy-Move forgery introduces a correlation between the original image segment and the pasted one which can be used as a basis for successful detection of this type of forgeries. Because the tampered image will likely be compressed and because of a probable use of the smoothing or other post processing operation, the segments may only match approximately not exactly. The authors give two different detection schemes: exact and robust matching those successfully detects duplicate regions in an image even the images are post processed following a copy-paste. Methods based on blur movement invariants and DWT, SVD, PCA based sorted neighborhood approaches are suggested in for robust detection of cloned regions in an image.

Splicing Detection Techniques

Digital splicing of two or more images into a single image is another commonly used image manipulation technique. When performed carefully, the borders between the spliced regions can be visually imperceptible. It is a popular way to distort the semantic content of an image so as to fool the viewer to misbelieve the truth behind a scene. Image splicing is a fundamental operation in image forgery and is characterized by simple cut-and-paste operation that takes a part of an image and puts it onto either the same or another image without performing any post-processing smoothing operation such as edge blurring, blending to it. By Image tampering, it generally means splicing followed by the post-processing operations so as to make the manipulation imperceptible to human vision [15].

METHODOLOGY

This system is used to detect tampered area of an image and to recover the lost information in the tampered zones [16]. Hash generation is used for detecting the tampered region and watermarked image is used for the recovery of the tampered zone. Watermarking stages includes source coding,channel coding,hashing. Block diagram for source coding Fig.2.

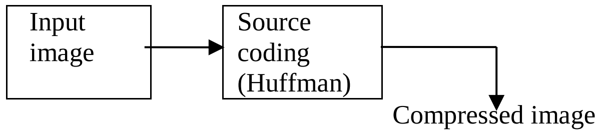

Fig.2.Source coding

In source coding Huffman algorithm which is used for compressing the original image. Watermarking process which takes the input and converted into gray scale image, processing is taken place only on that image. Compressed image is permuted then only the Channel coding is performed. The main reason for this the security. Permution also done at the output of the this. Block diagram for channel coding Fig.3.

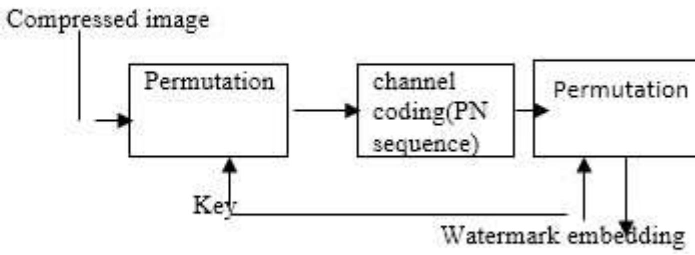

Fig.3.Channel coding

Hash is used for detecting the tampered region. These compressed data and hash are stored at LSB bit. Block diagram for hash generation Fig.4.

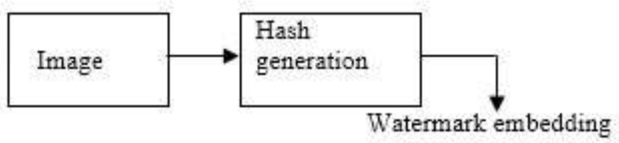

Fig.4. Hash generation

RESULT AND ANALYSIS

Implemented the watermark embedding of a scenery image cameraman.tif for the purpose of protection. The data is embedded on different LSB values and the corresponding variations shown in the image are verified. From the method we will be able to show that the noticeable distortion happening in the original image can be avoided by watermark embedding, since this technique preserves the quality of the original image. The recovery of the tampered image is also implemented. The result is as shown below.

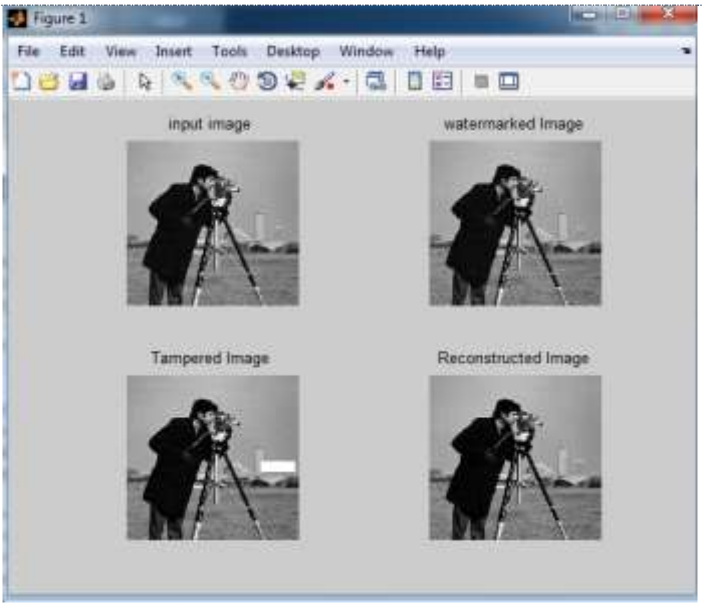

Fig.4. Digital image protection and self-recovery

In order to evaluate the performance of the watermarked images, there are some quality measures such as SNR, PSNR, MSE, AND BER.

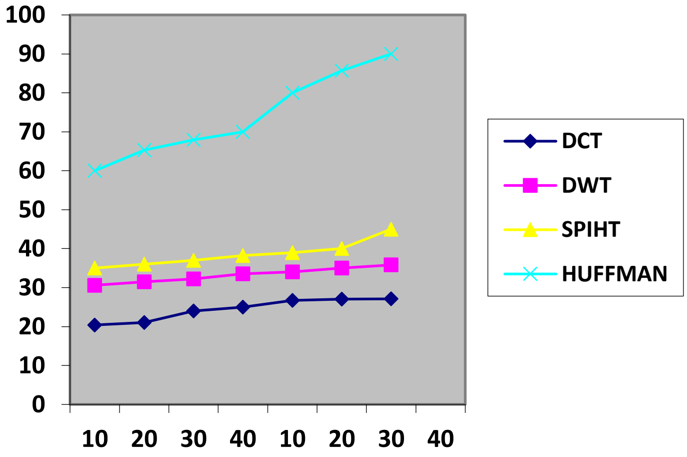

Fig.5. Result of different methods

X axis:-Tampering percentage
Y axis:-PSNR in recovered area

CONCLUSION

The Huffman code compression algorithm is used to source code the actual image. An 8×8 pixel in an image is splitted into Most Significant Bit (MSB) and Least Significant Bit (LSB). Further, a modified watermarking scheme is used to protect the original image from damaging/tampering. Then the LSB bits are divided into source encoder bits, check bits and channel encoder bits. This modified scheme uses the check bits present in the LSB bits to locate the tampered zone and the PN sequence channel coded bits are used to recover the image in that tampered area.

A tampering model is modeled to find the erasure error. This error is utilized by the PN sequence channel decoder in recovering the original image. In this paper, the implementation of encoder and decoder circuits is simple. The peak signal to noise ratio is high compared with the proposed method. A better image recovery is achieved using these techniques. In Future, various improvements in Huffman algorithm can be made in the areas of speed with high PSNR, resilience and memory requirement.

REFERENCES

[1] C. I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications," IEEE Signal Processing Magazine, July 2001, pp. 33-46.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, 2002.

[3] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk and E. J.Delp, "Advances in Digital Video Content Protection," Proceedings of the IEEE, Special Issue on Advances in Video Coding and Delivery, 2004.

[4] J. Sang and M. S. Alam, "Fragility and robustness of binary-phase-onlyfilter-based fragile/semifragile digital image watermarking," IEEE Trans. Instrum. Meas., vol. 57, no. 3, pp. 595–606, Mar. 2008.

[5] H.-T. Wu and Y.-M. Cheung, "Reversible watermarking by security enhancement," IEEE Trans. Instrum. Meas., vol. 59, no. 1, pp. 221–228, Jan. 2010.

[6] Wong P. W., Memon N.: Secret and Public Key Image Watermarking Schemes for Image Authentication and Oweship Verification, IEEE Transactions on Image Processing, 2001V01.10.(10):l593-1601.

[7] Neeta Deshpande, Snehal Kamalapur and Jacob Daisy,"Implementation of LSB steganography and its Evaluation for Various Bits",1st International Conference on Digital Information Management,6 Dec.2006pp.173-178.

[8] Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," Proc. IEEE Int. Conf. on Image Processing, Oct.1997, vol. I, pp. 548-551.

[9] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[10] Manoranjan Kr Sinha, Dr. Rajesh Rai, Prof. G. Kumar, "Digital Watermarking", International Journal of Computer Science and Information Technologies, vol.5, 2014, pp.6538-6542.

[11] M. Shensa, "The discrete wavelet transform: Wedding the a torus and mallat algorithms," IEEE Transactions on Signal Processing, vol. 40, no. 10, pp. 2464–2482, 1992.

[12] Mitchell D. Swanson, Mei Kobayashi, Ahmed H. Tewfik, "Multimedia Data Embedding and Watermarking Technologies", Proceedings of the IEEE, 86(6):10641087, June 1998.

[13] F. Deguillaume, S. Voloshynovskiy and T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack", Signal Processing, Elsevier, vol. 83, (2003), pp. 2133–2170.

[14] H. Farid, "Image Forgery Detection: A survey", IEEE Signal Processing Magazine, (2009) March, pp. 16-25.

[15] M. Mishra, "Digital Image Tamper Detection Techniques - A Comprehensive Study", Department of Information and Communication Technology Fakir Mohan University, Balasore, Odisha, India (2013**).**

[16] Saeed Sarreshtedari and Mohammad Ali Akhaee, "A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery," IEEE Transactions on Image Processing, vol. 7, no. 12, pp. 2266-227, July 2015.

CITE AN ARTICLE:

Biju, K., & S, R. K. (2017). DIGITAL IMAGE PROTECTION AND SELF-RECOVERY USING WATERMARK ALGORITHM. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(5), 143-149. doi:10.5281/zenodo.571749