A HYBRID APPROACH TO ENHANCE THE SECURITY OF IMAGE USING WATERMARKING THROUGH MODIFY SLT TECHNIQUES.

Sonali Kanotra, Prabhpreet Kaur

ABSTRACT

Image watermarking is the mechanism of hiding critical information in the form of logo image within original image. Information in the graphical form is represented with the help of watermarking strategies. Security concerns required updated technologies for reliability enhancements. To tackle the issue, modified discrete wavelet transformation is used in the proposed literature for watermarking. In modified approach blue component of the original images in LL band is used for decomposition using discrete wavelet transformation. The bits of information from the image are then merged within the original image. To extract the bits from the image, DWT coefficients in LL bands are calculated and then subtracted from watermarked coefficients. This will gives us original watermarked bits. In order to exhibit robustness and capacity proposed mechanism is distributed and embedded over the original image. Result is obtained in terms of peak signal to noise ratio and mean square error. Result shows improvement by 10% proving the worth of the study.

Keywords: Image watermarking, Modified DWT, PSNR, MSE.

INTRODUCTION

Image watermarking is the mechanism of embedding multiple images to enhance security of digital information. Techniques of watermarking are researched over by various researchers and image processing toolbox is used for facilitating watermarking process.[1] The problem of copyright can be overcome by merging multiple images before distributing digital information to the public. The watermarking process which is efficient will not degrade the quality of the host image. Embedded watermarked also should be visible to naked human eye. Furthermore the embedded watermark must be robust enough to tackle the issues of noise and attacks.

Late years have seen a quick development in the accessibility of computerized media content. Today, computerized media archives can be conveyed by means of the World Wide Web to countless without much exertion and cash. [2]Moreover, not at all like conventional simple replicating, with which the nature of the copied content is corrupted, advanced apparatuses can without much of a stretch create extensive measure of ideal duplicates of computerized archives in a brief period. This simplicity of computerized interactive media appropriation over the Internet, together with the likelihood of boundless duplication of this information, debilitates the protected innovation rights like never before. Hence, content proprietors are energetically looking for advances that guarantee to ensure their rights.

In the present period [3], [4]advanced security turns into the most smoking point because of its capacity to decrease the cost related with registering. Computerized registering gives the on request benefits like stockpiling, servers, assets and so on to the clients without physically obtaining them and the instalment is as per pay per utilize. Since image processing gives the capacity, diminishes the overseeing expense and time for association to the client however security and classification turns into the one of the greatest problems before us. To tackle the issue [5] slantlet transformation is used. The real issue with cloud condition is, the quantity of client is transferring their information on distributed storage so now and again because of absence of security there might be odds of loss of privacy. To beat these hindrances an outsider is required to anticipate information, information encryption, and trustworthiness and control unapproved access for information stockpiling to the cloud.

With the fast improvement of equipment and programming computerized security acquires the insurgency the business. It gives assets like computational power, stockpiling, calculation stage promotion applications to client on request through web. A portion of the cloud suppliers are Amazon, IBM, Google, Sales drive, Microsoft and so on. [6]Computerized processing highlights included asset

sharing, multi-tenure, remote information stockpiling and so on yet it challenges the security framework to secure, ensure and process the information which is the property of the individual, undertakings and governments. Despite the fact that, there is no prerequisite of information or ability to control the foundation of mists; it is dynamic to the client. It is an administration of an Internet with high adaptability, nature of administration, higher throughput and high processing power. Advanced registering suppliers send normal online business applications which are gotten to from servers through web program. Information security is the greatest issue in computerized security and it is difficult to determine it.

Watermarking approaches are classified either on the basis of frequency or spatial domains. Frequency and spatial domain watermarking techniques are described in the next section. Rest of the paper is organised as under: section 2 gives the literature survey, section 3 gives the proposed work, section 4 gives the performance analysis and results, section 5 gives the conclusion and future scope, section 6 gives the references.

2. LITERATURE SURVEY

The watermarking techniques are classified into frequency and spatial domain mechanisms. Frequency domain mechanisms include DCT and stegnography method.

2.1 DISCRETE COSINE TRANSFORMATION(DCT)

[7]DCT is an effective mechanism that provides image encryption. DCT is used to convert image from spatial domain to frequency domain.[8], [9] DCT is applied at source end from where information is to be transferred. Inverse DCT is applied at destination end to decode the transmitted information. The equation used for encryption at source end is given as

$$F(x,y) = \frac{1}{4} * C(u)C(v) \sum\sum f(x,y) * \frac{\cos(2\pi x + 1)}{16} \cos(2\pi y + 1)}{16}$$

Where c indicates cariears used to transfer the signals f is a function indicating frequency domain, u and v indicates range of values that are required to be transmitted.

At the receiver end inverse DCT is applied as under

$$F(u,v) = \frac{1}{4} * C(x)C(y) \sum\sum f(u,v) * \frac{\cos(2\pi x + 1)}{16} \cos(2\pi y + 1)}{16}$$

2.2 STEGNOGRAPHY METHODS

[10], [11]Stegnography uses images to store the text to be transmitted. The transmitted image is decoded at the receiver end using a key. The extra image space is used to store text information to be transmitted. The technique of extra space preservation is associated with digital images. In LSB stegnography, the image encryption is performed at the bit levels. The pixel intensity values are altered during encryption. In case of distortion, tradeoff exists between payload and distortion. Payload vary as distortion appear within the image. This distortion is a part of attack. [10], [12]Filtering mechanism accompanied with stegnography. Filtering mechanisms enhances the peak signal to noise ratio and eliminate distortion if any present within the image. stegnography is shown as under

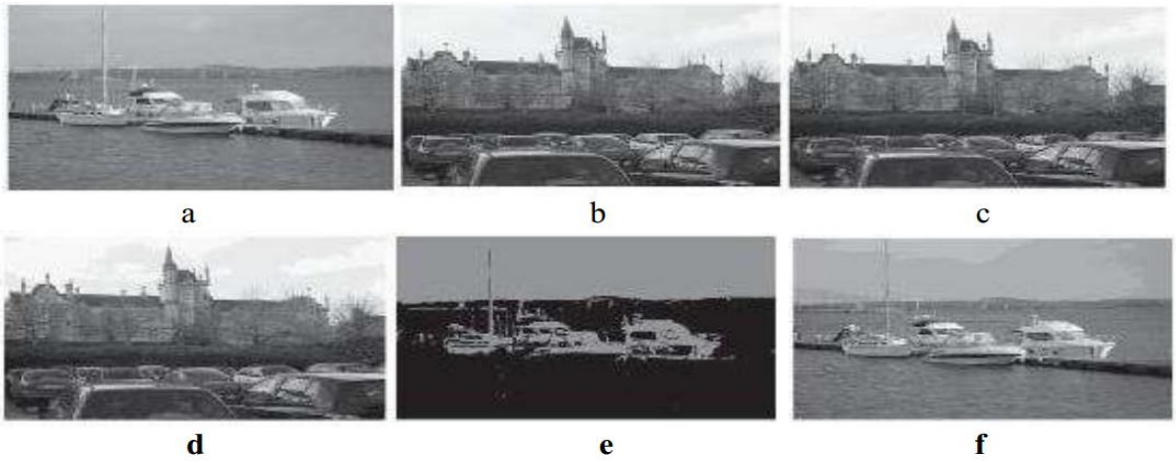

Figure 2: LSB Stegnography. a Image to be hidden b Carrier Image c First level of stegnography d Second level of stegnography e third level of stegnography f forth level of stegnography

[12], [13]Stegnography in general involves replacement of nosy component within image with the random secret message. In stegnography most common noisy components are least significant bits (LSBs). These LSBs are imperceptible and hence can be replaced by secret messages.

Most significant bits also contain some noisy components and hence they can also be used to encode secret messages. The proportion of image encryption is limited as compared to LSB stegnography. The MSB stegnography can replace LSB stegnography in case data to be transmitted is limited in quantity.

Spatial domain mechanism includes discrete wavelet transformation.

2.3 DWT

Discrete wavelet transformation is the mechanism in which discrete wavelets are sampled. Advantage of using this approach is temporal resolution of the image is not disturbed. Standardised wavelets that are used include Haar transformation. [14], [15]This transformation mechanisms stores input values and then pair them up. After pairing, difference is obtained. This difference is added to obtain summed value which is passed towards the destination. In addition daubechies wavelets are also commonly used which are based on the recurrence relation to generate finer samples of wavelets. The resolution of generated sample is twice than that of previous sample. This could lead to more accurate and reliable samples in watermarking which are less prone to attacks.

In proposed work, DWT with haar transformation are chosen for watermarking with the enhancement in terms of DWT coefficient in LL band. Next section gives the proposed system with methodology to be followed.

3. PROPOSED SYSTEM

The proposed system consists of Discrete wavelet transformation enhancement mechanism in order to achieve higher peak signal to noise ratio along with lesser mean square error. DWT coefficient in LL band is modified in proposed work. This indicates that blue component within the cover image is selected for distribution within the original image. Entire work of proposed system is divided into phases.

3.1 Watermarking image strength determination phase

In this phase a suitable static value is determined to strengthen the watermark to be used in watermarking process. Tuning factor can be determined by the use of following equation

$tuning_{factor} = \omega(i,j) + s$ equation 1

Tuning factor is calculated for each bit to be embedded within the original image. 'W' is the coefficient value within LL band and s is constant having value from (min)0.1 to (max)0.9.

3.2 Embedding bits within the original image

This phase embed the bit within the original image. Blue component of the original image is chosen for embedding. Blue components are subdivided into four bands by the application of 2D Dwt. These four bands includes approximation, horizontal, vertical and diagonal band. Random value generator generates a unique random value corresponding to blue regions within the original image. The band is thus selected randomly to merge a single bit within the band given by following equation

$\omega'(i,j) = w(i,j) + b(i,j) * s * tuning_{factor}$ equation 2

where's' is the signal strength and w gives the location where embedding is to be performed. To embed multiple bits into the original image, a logo image is considered and divided into multiple parts by applying the 2d DWT and blue component in the original images again are partitioned into four bands. Random values are used to spread the logo image contents within the image. The image is so obtained is watermarked image.

3.3 Image extraction process

To extract the embedded bits, w^t is decomposed two times using dwt transformation. The DWT coefficients in four bands in level 2 are replaced by 0s. After that inverse transformation is applied to extract prediction of the original image along with cover image. These prediction coefficients are subtracted from watermarked coefficients to obtain the original and cover image.

$Orignal(i,j) = w'(i,j) - b(i,j)$ equation 3

b(i,j) is the original coefficient in the LL band. By the implication of this third phase, origna and cover image becomes separated.

Methodology to be followed is given as under

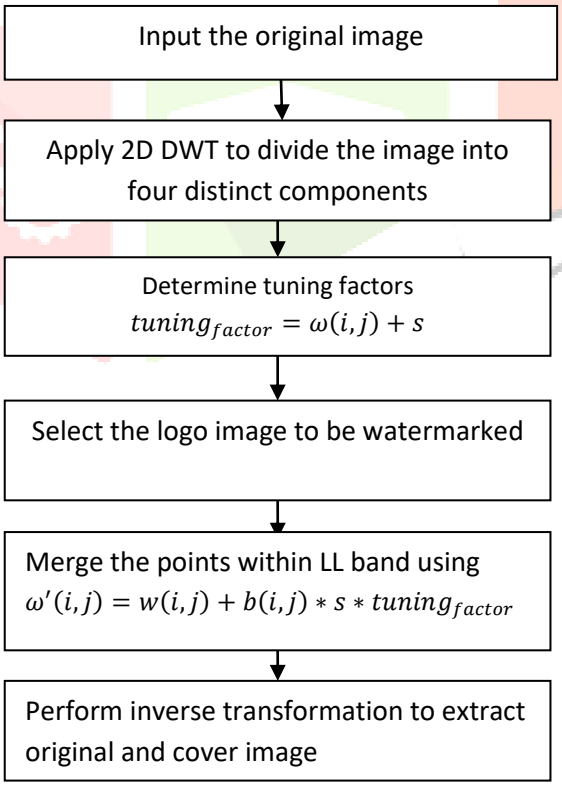

Figure 2: proposed Methodology

Result and performance analysis suggests better outcome in terms of peak signal to noise ratio along with mean square error.

4. RESULTS AND PERFORMANCE ANALYSIS

Digital watermarking is a productive strategy to ensure copyright and responsibility for data. Digital watermarking is the strategy for inserting digital data in any type of sight and sound information, for example, picture, sound, video, and so forth .It is a technique for concealing one mystery message in another message. In prior days watermarks were utilized as trademark or logo for showing the responsibility for particular product. But in conventional techniques for digital picture watermarking, the surface of unique picture gets mutilated pretty much.

In proposed system noise is handled by component capable of introducing clarity within the image though filtering. In the wake of getting the clearness watermarking is forced. The picture information introduced to the reproduction is of .jpg and .png type. Results as far as MSE and PSNR is acquired the coveted reproduction.

Table 1: Comparison of Mean square error

Image set	MSE Existing	MSE Proposed
Image1	14.0869	7.04345
Image2	15.7442	7.87209
Image3	132.03	66.015
Image4	14.0869	7.04345
Image5	31.7646	15.8823

Plots of result from the comparison table is as under

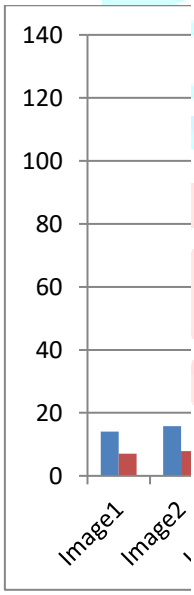

Figure 1: Plots of MSE

Comparison of PSNR is given as under:

Table 2: Comparison in terms of peak signal to noise ratio

Image set	PSNR Existing	PSNR Proposed
Image1	18.3383	39.6869

Image2	18.0968	39.2039
Image3	13.479	29.9684
Image4	18.3383	39.6869
Image5	16.5727	36.1557

Plots of PSNR with existing and proposed mechanism are given as under:

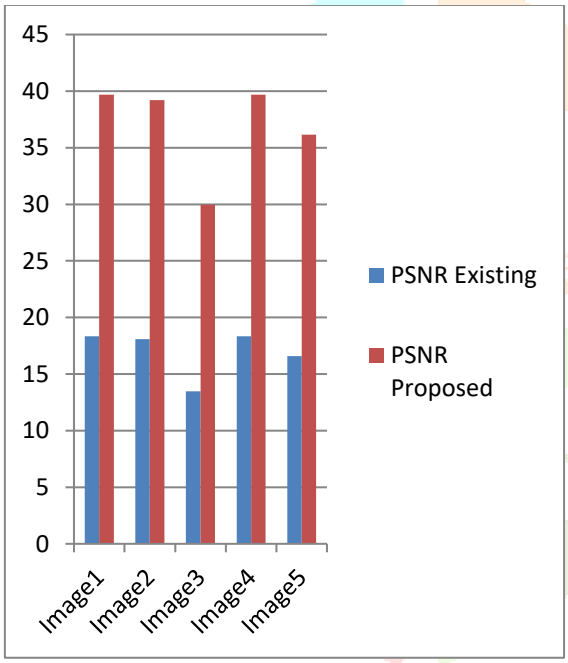

Figure 2: Plot of PSNR

Result in terms of PSNR and MSE of proposed system is better proving the worth of the study.

5. CONCLUSION AND FUTURE SCOPE

Transmission of information using graphical user interface has become need of the hour. Proposed system using new technique of DWT with the modification to LL band produce efficient watermarking image. It tackled the noise automatically if introduced within the image. Due to which original image is extracted without any distortion. LL band embedding and extraction follows random number generator mechanism. This random number generator uniformly distributes the cover image over the original image. Inverse transformation yields the original and cover image back again. The proposed system gives the betterment in results by 10%.

In future, singular valued decomposition along with DWT can be used for image watermarking to transmit digital information over the network.

6. REGERENCES

[1] G. Gupta, A. M. Joshi, and K. Sharma, “AN EFFICIENT ROBUST IMAGE WATERMARKING BASED ON AC

PREDICTION TECHNIQUE USING DCT TECHNIQUE Watermarked image," vol. 9102, no. August, pp. 1055–1059, 2015.

[2] A. Chitla and C. M. M, "Authenticating Medical Images with Lossless Digital Watermarking," *ijmcr*, no. April, pp. 291–296, 2014.

[3] P. Parmar and N. Jindal, "Image Security with Integrated Watermarking and Encryption 1 1 2," vol. 9, no. 3, pp. 24–29, 2014.

[4] T. Bathinda, "Invisible Video Multiple Watermarking Using Optimized Techniques," 2016.

[5] R. T. Mohammed and B. E. Khoo, "Image watermarking using slantlet transform," *ISIEA 2012 - 2012 IEEE Symp. Ind. Electron. Appl.*, pp. 281–286, 2012.

[6] R. K. Sheth and V. V. Nath, "Secured digital image watermarking with discrete cosine transform and discrete wavelet transform method," *2016 Int. Conf. Adv. Comput. Commun. Autom.*, pp. 1–5, 2016.

[7] A. Kaur and J. Kaur, "Comparision of Dct and Dwt of Image Compression Techniques," vol. 1, no. 4, pp. 49–52, 2012.

[8] M. a. Faizal, H. B. Rahmalan, E. H. Rachmawanto, and C. A. Sari, "Impact Analysis for Securing Image Data using Hybrid SLT and DCT," *Int. J. Futur. Comput. Commun.*, vol. 1, no. 3, pp. 309–311, 2012.

[9] Z. J. Xu, Z. Z. Wang, and Q. Lu, "Research on Image Watermarking Algorithm based on DCT," vol. 10, pp. 1129–1135, 2011.

[10] X. Pan, B. Yan, and K. Niu, "Multiclass Detect of Current Steganographic Methods for JPEG Format Based Re-stegnography," no. experiment 1, pp. 2–5.

[11] K. Saranya and A. Professor-i, "Modern Applications of QR-Code for Security," no. March, pp. 1–5, 2016.

[12] V. Saravanan and A. Neeraja, "Security issues in computer networks and stegnography," *7th Int. Conf. Intell. Syst. Control. ISCO 2013*, pp. 363–366, 2013.

[13] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali, and M. Naeem, "An improved image steganography technique based on MSB using bit differencing," *2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016*, pp. 265–269, 2017.

[14] A. Mtech and A. Dwt, "Image security using watermarking based on DWT-SVD and Fuzzy Logic," 2015.

[15] M. Imran and A. Ghafoor, "A PCA-DWT-SVD based Color Image Watermarking," pp. 1147–1152, 2012.