International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

An Efficient Watermarking and Key Generation Technique using DWT Algorithm in Three-Dimensional Image

R. Saikumar, D. Napoleon

Abstract*:Discrete Wavelet Transform is the algorithm which can be used to increase the contrast of an image for better visual quality of an image. The histogram value for original image with highest bins is taken for embedding the data into an image to perform the histogram equalization for repeating the process simultaneously. Information can be embedded into the source image with some bit value, for recovering the original image without any loss of the pixels. DWT is the first algorithm which has achieved the image contrast enhancement accurately. This approach maintained the original visual quality of an image even though themessage bits are embedded into the contrast-enhanced images. The proposed work with an original watermarking scheme based on the least significant bit technique. As a substitute of embedding the data into a simple image as watermarking, least significant bitmethod by utilizing the three wavelets transform is applied in the proposed system in order to enhance the embedding technique using spatial domain. For security, the Huffman coding has used to secure the data embedded into a host image, which can convert the secret message sequence into bit sequence for least significant bit operation. DWT can analyze the signal at multiple resolutions and it can divide the image into two types of quadrants as high and low-frequency quadrants. Here dividing an image into low and high it makes the information to hide.

Index Terms: DWT; Digital Image Processing; Huffman coding; Watermarking.

I. INTRODUCTION

The digital multimedia needs more security while transmitting over the network as image, audio, video, and text nowadays. There is an enormousnumber of these data are transmitted through network simultaneously. And the channel where these data are transferred is unsecured and constrained in bandwidth. To overcome all these demerits in transferring the data compression and encryption is the best method for transferring the multimedia data more secure through the internet.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
R. Sai Kumar*, Research Scholar Department of Computer ScienceBharathiar University, Coimbatore, Tamilnadu, India.Email-saicompsci@gmail.com
Dr. D. Napoleon, Assistant Professor Department of Computer Science Bharathiar University, Coimbatore, Tamilnadu, India.Email-mekaranapoleon@yahoo.com

The security has been applied for the data transferred through the network as cryptography and steganography. The steganography is the powerful technology applied for hiding the information that cannot be identified by the third party. Cryptography provides the security to the data transferred over internet, which creates an encrypted form of plaintext. Here the third party can see only the encrypted text, but the original information cannot visible to that intruder. To obtain a better security andconfidentiality the combination of both the Cryptography and Steganography is utilized in the proposed system. Compressive sensing is used to obtain compression and encryption of the data is obtained by compressive sensing. It is a novel technology used to compress the data at a higher rate than the conventional method. The compression and encryption are achieved by a single linear measurement step through a measurement matrix, which can be generated by the secret key. This key can be shared only among the sender and the receiver at the time of sending and receiving data as a multimedia file.

II. LITERATURE REVIEW

Y. Sridhar et al: An author says about the unique structure about the scalable coding for PRNG images which have been encrypted. At the stage of encryption, the values of a source pixel are masked by modulo addition with pseudo-random numbers to provide the secret key. During the decryption there are some data sets with multiple resolution construction [4]. Then, quantized encrypted image and the coefficients of the data are observed as a set of bit streams. From the receiver side, while a cipher text is decrypted to provide the uneven data about the source content, then the quantized coefficients is applied to recover the original content. Due to the classified coding technique, the principal of source content with great quality can be reconstructed when more bit streams are received.

Raj et. al., Analysed the Discrete Fourier Transform and Adaptive Filtering methods for implementing the encryption based on the holomorphic properties of a cryptosystem method. This reduces the computation complexity and the encrypted data size effectively [5]. The proposed technique is a combination of encryption and data hiding. A part of required data of a plain signal is encrypted for securing data, balance data are used to carry buyer and seller protocols.

The fingerprint information is embedded into an encrypted version to ensure that the seller cannot able to identify the buyer's watermarked version. There are N numbers of stages on compressing the information for encrypting an image has been also presented.

Michal Vargaet. al.,Presents a review on latest trends in 3D computer vision. In image processing, the research has advanced significantly over the past decade [6]. The author reviews the basic and advanced approaches of 3D image acquisition and procedures for storing, processing and understanding this data. The main focus of this research is autonomous mobile robotics and automated industry. Along with the strengths and weaknesses, several passive and active optical range imaging approaches are reviewed. Some of the most common range image processing methodology and their structures is also described.

Neha Verma et. al., The proposed work of the author implements that the method of watermarking for the purpose of sharing the digital data while the transmission over the internet using spatial domain approach and LSB techniques, spread spectrum, predictive coding schemes, patch work techniques and transform or frequency domain approach. Here the host image can be decomposed into N-levels using pyramid L-level technique. This mechanism is considerable to apply in a real-world application because it can directly capture the applied watermark from the watermarked image devoid of the source image.

Amrita Sengupta, Sanjeev Ghosh. Discussed about the significance of security in every single application on the internet is a strong encouragement to focus in the area of data Security. When the information needs to transmit from one source to another it is necessary to compress the data and hidethat information for security before sending to the destination [7]. Because it is insecure in transferring the data over the internet with any security among third-party theft may occur. In this proposed system, the process of securing the information is different from other works. That is the compression is done later and encryption of data done earlier. Due to coding with side data principles, this reversal order is possible without any loss. The researcher implements compression of encrypted data in order to prove the theoretical possibility of these reversal operations. Further disorder theory is developed to overcome the difficulties present in encryption. Eventually, the results are compared with chaotic based encryption method followed by SPIHT algorithm.

Navdeep Goel et. al., From the research work, the author conveys that the watermarking has done in the images using wavelet functions of the discrete wavelet transformation where the DWT and decomposition process have taken place. With the use of DWT, the frequency may vary and it cannot make any changes of data from the signal. DWT change the host image into partition image of various spatial domain and signal. The host image can be decomposed into N levels and retrieved by constructing all the information from the sub-images such as Haar, Symlet, Coiflet are the DWT wavelets associate together.

Jadhao et. al., An author explains that the image has encrypted for embedding the data for digital watermarking which can be used for QR Code. This method gives assurance to the users that the copyrighted content may not be copied from the original document from network is easily analysed. Because the degradation of the watermarking is decreased for quality of an image [8]. There are lot of methods are there to hide the data, but watermarking is the more secure technique to hide the data with the help of images for secure transmission even in the unsecured network.

Shruthishree et. al., sketched some of the significant concepts of medical image processing. It is highlighted that none of these issues has been satisfactorily solved, and all of the algorithms described by the researcher are open to considerable improvement. Particularly, segmentation remains a rather ad hoc technique with the improved results being received via interactive programs with input from the user. Still, progress has been made in the field of medical images analysis, the researcher thanks the improvements raised in several areas. Curvature driven flows method is a proven tool for a number of image processing tasks and have definitely had a major impact on the technology base.

VairaprakashGurusamy et al., Stated as Image segmentation and universal segmentation algorithm has a bright future and has become the focus of contemporary research. Accordingly, image segmentation is affected by several factors such as texture and image content, homogeneity of images and spatial characteristics of the image continuity. The researcher discussed various techniques of image segmentation and presents the proposed image segmentation algorithms and classification techniques.

III. METHODOLOGY

A Discrete Wavelet Transform (DWT) conveys the finite sequence of data points into the sum of Wavelet methods oscillating at various frequencies [1]. DWTs are significant to several applications in science and engineering, from lossy compression of audio and images as multimedia components to spectral functions for the mathematical solution of partial differential equations.

The fundamental operation of the DWT is given below:

- The source image is P by Q
- F (x, y) is the depth of the pixel in row x and column y;
- F (n, m) is the DWT coefficient in row a1 and column a2 of the DWT matrix.
- For several images, much of the signal energy lies at less frequencies these appear in the upper left corner of the DWT.
- Compression is obtained because the lower right values denote higher frequencies are often small - small enough to be neglected with few visible distortions.

- The input for DWT is an 8 X 8 array of integers. This array has each pixel's gray scale level.
- 8-bit pixels have levels from 0 to 255.

A Least Significant Bit (LSB) is the basic watermarking method to embed a watermark in the LSB of some randomly selected pixels of the cover image [2][3]. The procedure of LSB is given below.

1) Change RGB to grey scale image.
2) Compute double precision for image.
3) Swap most significant bits of watermark image to low significant bits.
4) Assign the least significant bits of host image to 0.
5) perform step 3 of watermarked image to modified step 4.

Example of LSB watermarking:

		1	0	0	0	1	1	0	1
Pixel Value									
							0	0	1
Secret Data									
		1	0	0	0	1	1	0	0
Changed Pixel Value									

Fig 1. LSB TECHNIQUE

LSB is the basic spatial domain method, as it carries less appropriate data and their changes do not cause visible modification. The embedding of watermark in LSB of randomly selected pixels of the source image is very simple. An image is given, where each pixel of image is denoted by an 8-bit stream, the watermarks are applied in the LSB, of selected pixels.

IV. PROPOSED METHOD

In the proposed scheme, the content owner firstly masks all pixel values in the original uncompressed image to get an encrypted image and provides the encrypted data to the channel provider. If the bandwidth is enough, the channel provider transmits the encrypted data. Otherwise, the channel provider sends a "bandwidth-insufficiency" message to the content owner, and then the content owner generates the auxiliary information according to the original and encrypted content and provides it to the channel provider. The auxiliary information (AI) is made up of two parts that will be respectively used for data compression and image reconstruction.

Authentication - To protect the authenticity of multimedia images, several approaches have been proposed. The cryptography method is not completely secured here. It can be breakable and semi- breakable of watermarking image where that image has some hidden information. These may happen depending upon the content feed into the image for security. The main scope of this paper is to present a survey and comparison work of emerging techniques for image authentication. The cryptography methods are classified according to the service they provided, that is strict or selective authentication, localization and reconstruction capabilities and robustness against different desired image processing operations.

Selecting Image – After some changes occurred in an image then add that changed or hidden sub-image into the original image. Suppose if the sub-image could not add into the original image automatically, make the encryption process by hiding the content by compression and then merge it into the sourced image. In case if we have any conflicts, we need to create images from the original image with some compatibility changes and then merge the sub-image into the original image.

Embedding the watermarked content -The steps of the proposed watermarking methodology is described as follows:

1. The image I have selected and DWT technique has applied to the original image.
2. Key has selected as K to generate QR code as a secret key.
3. Simple XOR operation is used to encrypt the QR code and Watermark, E (I, j) =W (I, j) Θ QR (I, j)
4. By applying simple condition encrypted Watermark is embedded in the original image, IF(E(I,j)==0)
5. Then apply Inverse DWT on the embedded watermarked image, WI (I, j) =IDWT I(I, j))

GENETIC ALGORITHM BASED APPROACH:

This approach can be used for the techniques known as image segmentation, classification, enhancement of the image, feature extraction and generation of an image. The genetic approach is used for the protection of the information used in the medical images. And also, the encryption method has helps to protect the image from different attacks called entropy attack, plaintext attack and brute-force attack. The genetic algorithm-based image steganography process makes the quality of an image and executes good embedding and PSNR values as a result.

DCT APPROACH

The discrete cosine transform has some basic set of cosine functions in it. It can be used to convert the signal to frequency components and also used for compression of an image. The DCT-Haar algorithm used to remove the noises from an image and introduces the quality measurement. The test image has some features like extraction for the improvement of the quality of the image [9] [10]. The most popular technique for image compression, over the past several years, was Discrete cosine transform (DCT). Its selection as the standard for JPEG is One of the major reasons for its popularity. DCT is used by many Non-analytical applications such as image processing and signal-processing DSP applications such as video conferencing.
The DCT is used in transformation for data compression. DCT is an orthogonal transform, which has a fixed set of basis function. DCT is used to map an image space into a frequency.

GENERATING THE TOKEN KEY

Here, the token key has generated by the combination of frequency and the binary value of an energy from the extracted vertices and faces of the source image. This technique is derived from the below-mentioned method:

Today the Modern cryptographic systems include the method called symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as RSA). A symmetric-key algorithm which has used to have a single shared key which keeps the data secure with this secret key. Public-key algorithms are used both the combination of public key and private key. The public key is common for to anyone A sender encrypts the data with the public key, then the user who has private key can only decrypt this data. Since, the public-key algorithms tend to be slower than symmetric-key algorithms, modern cryptography systems such as TLS and SSH uses a combination of two: one party receives the other's public key and encrypts a small region of that data. The remainder of the conversation uses a symmetric-key algorithm for encryption.

Computer cryptography uses integers for keys. In some cases, the keys are randomly generated using a random number generator (RNG) or pseudo-random number generator (PRNG). There are some computer accessing algorithm which produces the data to appear randomly under the analysis of content from an image. PRNG is the method which uses the system entropy to seed the data whichproduces better results, and it makes the third- party users to guess the PRNG. There are some other ways to generate the randomness to utilize the information from outside the system. VeraCrypt is a software which can be used for disk encryption which utilizes user mouse movements to generate unique seeds, in which users are encouraged to move their mouse infrequently.

WATERMARKING APPROACH

The watermarking approach can be used to detect the copyright protection and tracking the digital content are copied from the copyrighted files are the very big issue [11] [12]. To overcome this problem, watermarking is the best solution to protect the duplicate content from the copyrighted document. Some normal watermarking is visible to the human vision such as company logos, TV channel logo, etc. and advanced watermarking technique are not visible to the human's vision, because the watermarked content is protected with some mathematical calculations. There is some transformation technique are used for encryption of an image as follow:

- Wrapping method
- Fast Fourier Transformation algorithm.

These are the two algorithms which can be used to protect the content from the unauthorized access with the help of watermarking to the digital content [13] [15].Digital watermarking consists of several techniques used for protection of the digital content. The digital image watermarking falls in two main broad categories:

- Spatial domain techniques
- Frequency domain techniques

V. RESULT

Fig a) Input Image

Here, an image can be taken as three-dimensional image with .OBJ file format. There are a lot of 3D formatted images which is readable for 360-degree angle. The rabbit image has taken for the proposed system and the data have compressed, encrypted and then hidden into the source image with some token. The key has been accessed only from the sender and receiver side. Without any awareness about token key, the user or the third party cannot access the hidden data from the image.The histogram is nothing but the technique which can be used for adjusting the intensity of an image to enhance the contrast of an image.

The above figure explains that, the output image after the histogram equalization has processed. The histogram is the type of bar plot for plotting thenumeric data which graph the data into a bin. Bins are nothing but the coupling of the data together and divide into the series of intervals and the values fall into each interval have been calculated.

Fig b) Secret Key

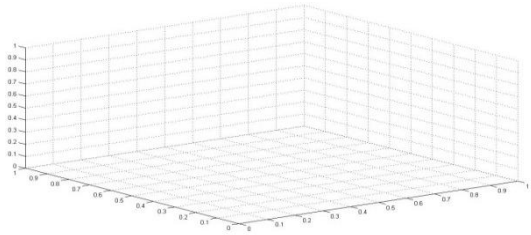

Fig c) Three- Dimensional Image at Sliced View

A three-dimensional file format has implemented in the proposed research for watermarking and it can be sliced into N numbers of sections to hide the data into the three-dimensional image file format.

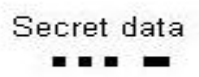

Fig d) Hidden Data

The data has some secret key which hides an information into the 3D file as shown in above figure. An information can be encrypted and it cannot be accessed without decrypting the image without unaware about the secret key. Then, the data hidden successfully into an image with encrypting technique using some image processing techniques where the image has reconstructed and the original 3D image has recovered after the successful decryption of the data. The below image shows that the data has extracted from the 3D formatted image and the original image can be reconstructed without any pixel loss.

Fig e) Original 3d Image Received at Destination

PSNR is a method to check the quality of an image which has reconstructed afterdecryption. The below equation is used for processing:

$$PSNR\ (db) = 10 * log_{10}[\frac{[255]^2}{\frac{1}{ST}\sum_{i=0}^{S-1}\sum_{j=0}^{T-1}(C(s,t) - WD(s,t))}]$$

The mean square error (MSE) have reached here with the proposed work as 1.9851 as compared with existing works and the PSNR2 value as 39.2340202. The proposed system shows the error accuracy lower by comparing with existing.

$$MSE = \frac{1}{S * t}\sum_{ii=1}^{S}\sum_{j=1}^{t}[C(S,t) - WD\ (s,t)]$$

Table 1: Performance results in terms of PSNR & MSE

SL.NO	METHOD / IMAGE	Image 1		Image 2		Image 3	
		MSE	PSNR	MSE	PSNR	MSE	PSNR
1.	2D DWT	1.703	45.85	0.443	51.692	0.321	53.087
2.	3D DWT	1.98	39.23	0.09	58.31	0.16	55.70

Table 2. Performance Results for 2-Dimensional Wavelet Transform

2D Images	Image 1		Image 2		Image 3	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
	1.7036	45.851	0.4439	51.692	0.3219	53.0872

The proposed system has implemented the novel DWT approach with the property of digital watermarking with secret key generation technique. Generally, the two peaksin the histogram are taken for data embedding so this process is repeated simultaneously to perform histogram equalization.

Table 3. Performance Results of Proposed 3-Dimensional Wavelet Transform

3D IMAGES	Image 1		Image 2		Image 3	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
	1.98	39.23	0.093	58.316	0.160	55.702

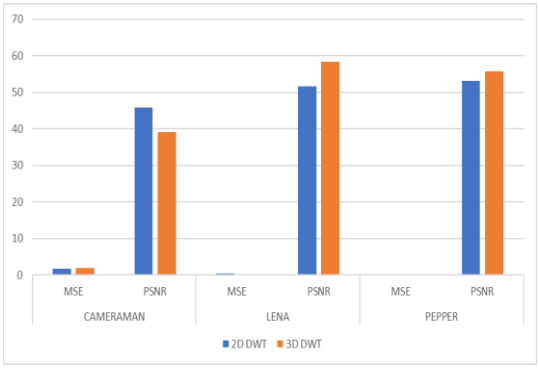

Fig 5.1.2 Comparison of 2-Dimensional DWT with 3-Dimensional DWT

VI. CONCLUSION

In order to secure the data, 3D watermarking technique has been implemented in the proposed research work. In this proposed work .OBJ extension file format watermarking technique is used to produce the better result. The data is hidden into the image as watermarked content and it is extracted successfully without any loss of the data and also the loss of pixel. The error rate is low in the proposed research work while comparing with the existing methodology. The experimental results have shown that, the contrast of an image can be enhanced by dividing into N number of histogram peaks pair by pair. Compared with the special MATLAB functions, the visual quality of the contrast-enhanced images generated by our algorithm is better conserved. Also, the original image can be exactly recovered without any additional information and also without any data loss. Hence the proposed algorithm has made the image contrast enhancement reversible. Improving the algorithm robustness, and applying it to the medical and satellite images for better visibility, will be our future work.

REFERENCES:

1. A. Furqan and M. Kumar, "Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB," in IEEE International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2015.
2. D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto and C. A. Sari, "Fast and Efficient Image Watermarking Algorithm," in International Conference on Cyber and IT Service Management (CITSM), Denpasar, 2017.
3. N. Narula, D. Sethi and P. Pratim B, "Comparative Analysis of DWT and DWT-SVD Watermarking Techniques in RGB Images," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 8, no. 4, pp. 339-348, 2015.
4. L. Samira, S. Mohsen, and F. Mahmood, "A New Robust Watermarking Scheme Based on RDWT-SVD: Embedding data in all sub bands," in International Symposium on Artificial Intelligence and Signal Processing (AISP), Tehran, 2011.
5. C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Robust and Imperceptible Image Watermarking by DC Coefficients Using Singular Value Decomposition," in International Conference on Electrical Engineering, Computer Science, and Informatics (EECSI), Yogyakarta, 2017.
6. A. Winarno, D. R. I. M. Setiadi, A. A. Arrasyid, C. A. Sari, and E. H. Rachmawanto, "Image Watermarking using Low Sub band based on 8×8 Sub-block DCT," in International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, 2017.
7. T. H. Nguyen, D. M. Duong, and D. A. Duc, "Robust and high capacity watermarking for image based on DWT-SVD," in IEEE RIVF International Conference on Computing & Communication Technologies - Research, Innovation, and Vision for the Future (RIVF), Can Tho, 2015.
8. S. Sirmour and A. Tiwari, "A Hybrid DWT-SVD Based Digital Image Watermarking Algorithm for Copyright Protection," International Journal of P2P Network Trends and Technology (IJPTT), vol. 6, pp. 7-10, 2014.
9. W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi and C. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 15, no. 4, pp. 1987-1995, 2017.
10. S. Nishane and P. V. M. Umale, "Review on Image Watermarking Techniques," International Journal of Innovative Science, Engineering & Technology, vol. 5, no. 3, pp. 1530-1532, 2015.
11. H. Gao, L. Jia, and M. Liu, "A Digital Watermarking Algorithm for Colour Image Based on DWT," TELKOMNIKA, vol. 11, no. 6, pp. 3271- 3278, 2013.
12. P. Shah, T. Meenpal, A. Sharma, V. Gupta and A. Kotecha, "A DWTSVD Based Digital Watermarking Technique for Copyright Protection," in International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, 2015.
13. A. Susanto, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hybrid Method using HWT-DCT for Image Watermarking," in 5th International Conference on Cyber and IT Service Management (CITSM), Denpasar, 2017.
14. Shuchi Sirmour. et al, "A Hybrid DWT-SVD Based Digital Image Watermarking Algorithm for Copyright Protection", IJPTT – Vol: 6 – Mar 2014 ISSN: 2249-2615.
15. Anuradha .et al, "DWT Based Watermarking Algorithm using Haar Wavelet", IJECSE, ISSN- 2277-1956.

AUTHORS PROFILE

R. Sai Kumar, Research Scholar Department of Computer ScienceBharathiar University, Coimbatore, Tamilnadu, India.Email-saicompsci@gmail.com

Dr. D. Napoleon, Assistant Professor Department of Computer Science Bharathiar University, Coimbatore, Tamilnadu, India.Email-mekaranapoleon@yahoo.com