3D (.Obj) Image Watermarking and Key Generation Using Dwt Algorithm

J.Jansi Rani, S.Anusuya, C.Senthamilarasi

Abstract: Digital media like images ,3D models audio and video can be used to embed signals in digital form. This process is popularly known as Digital Watermarking.The digital watermarking process is done by different methodologies such as steganography and by cryptography. The steganography method is used to hide the data and the cryptography method is used to encrypt the data into desired format. In this paper we proposed the method of cryptography and DWT (Discrete Wavelet Transform) algorithm for hiding the data and to generate a secret key for the data transmission. The data is embedded in a 3D real time object (.obj). The frequency and energy of the image pixel is calculated by DWT algorithm and by doing XOR operation the secret key will be generated by cryptography method. The 3D image is divided by vertical splicing technique. The data is embedded into an image in the form of binary data as 0's and 1's.

Index Terms: Cryptography, DWT, Vertical Splicing, 3D obj image.

I. INTRODUCTION

Digital watermarking is a subfield of Digital signal processing. It helps to hide the content of information in an audio, video, image and in 3D models. The Digital watermarking is the encryption and decryption of data into different form for security transmission. It involves two types of operations such as 'embedding the information as watermark' and 'extraction' based on the spatial and frequency domain. Watermarking may be in the form of image, text, authentication key, password etc. In recent years, there is an extraordinary amount of file transfer, data transfer through the internet to the world wide. To avoid duplication and manipulation of data, it is necessary to verify the original content before transmission through the internet. So an embedding of invisible data into original data in the form of multimedia streams for protection and for security purpose. Security and confidentiality is important during data transmission to avoid data loss and to avoid the security threads in transmission. Normally, digital watermarking techniques include steganography and cryptography for hiding the data. Steganography is done only to hide the data in an image or in other file. Cryptography is done to hide the data in an image in different form in an image or in the other file formats by the generation of secret key. To prevent the detection of encrypted data using steganography, the cryptography algorithms has been used. Watermarking and cryptography are closely related but the watermarking is different from encryption. The watermarked data is stored and transmitted but decrypted in the receiver side. Based on the human perception it is divided as fragile and robust. Based on the types of application, it is classified as source based and destination based. Source based if it is used for authentication and for ownership identification. Destination based to determine the owner in case of illegal issues. The major requirements of watermarking are robustness, capacity and transparency. This system is applicable to both unicast and multicast applications. Cryptographic mechanism is used for network security issues which help to prevent the data loss during transmission over the network. It involves encryption and decryption operations. Encryption is the process of converting the plain text into cipher text (hidden text) to secure the data from the intruders. The data cannot be viewed by the intruders without the authentication key. With the help of private key it is routed over the network to the receiver. Decryption is the process of converting the cipher text (hidden text) into plain text (unhidden text) with the help private key. The encryption and decryption process is shown below:

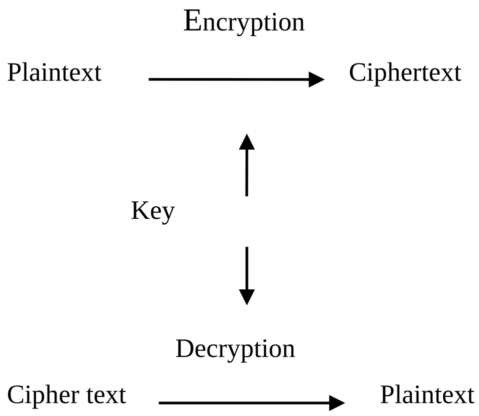


Fig.1 : Cryptography flowchart

II. DISCRETE WAVELET TRANSFORM

Recent research work and advancement in the areas of image processing have much interest in the field of content retrieval and perceptual. Human perceptual includes shape, pixel size, brightness, contrast, intensity etc. Discrete wavelet transform is known to be a very useful tool in signal processing. It converts a discrete time signal into corresponding discrete wavelet representation. It provides multiple resolution rate, scalability, degradation of the signal due to presence of noise.

Manuscript published on 30 September 2019.
*Correspondence Author(s)

J.Jansi Rani,,Department of Electronics and Communication Engineering,Anna University, Sri Krishna College Of Engineering and Technology, Coimbatore, India.
S.Anusuya, Department of Electronics and Communication Engineering, Anna Universit, Ramakrishna College of Engineering and Technology,Trichy, India.
C.Senthamilarasi, Department of Electronics and Communication Engineering, Anna University, Sri Krishna College Of Engineering and Technology , Coimbatore, India.

Retrieval Number: I8667078919/19©BEIESP
DOI: 10.35940/ijitee.I8667.0981119
Journal Website: www.ijitee.org

It increases the accuracy by increasing the level of transformation. It can be used for image compression, digital watermarking and for edge detection. In 1-D DWT the input sequence is divided into low pass and high pass sequence. In 2-D DWT, the input is decomposed 4 sub bands namely low-low band, low-high band, high-low band, and high-high band. The representation of DWT is depicted as:

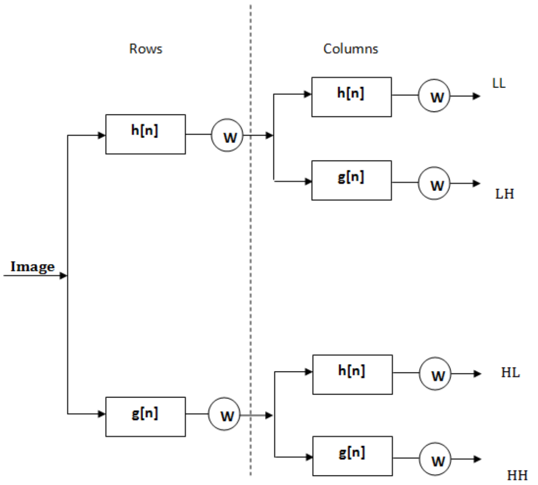


Fig .2: Discrete Wavelet Transform

The basic operation involved in DWT is explained as follows:

1.The input image is represented as N by M;
2.F (i,j) is the value of the pixel in row i and j;
3.The DWT coefficient in row k1 and column k2 of the DWT matrix is denoted as F (u, v) .

For large number of images,significant amount of the signal energy falls at low frequencies which in the upper left corner of the DWT. As the values in lower right coner represent the higher frequencies, compression can be achieved.This is possible since these values are small enough to get neglected with little or no visible distortion. The 8 by 8 array of integers has been applied as input to DWT. This array represents gray scale level of each pixel which have levels starting from 0 to 255.

III. LITERATURE SURVEY

The term Watermarking represents the procedure of embedding digital signals into another digital formats which include images, audio, video, or 3D models . Steganalysis is the finding of watermarks hidden into these digital signals [1]. One of the efficient methods of encryption and decryption of watermark is the simulation process using Discrete Wavelet Transform (DWT). Using this method, the embedded image can be completely recovered. But, Sometimes it causes restriction to access the original image[2]. Steganography is used efficiently to hide secret messages in a host media which is otherwise called as cover media. But, noise is high and the amount of data that can be hidden is considerably less[3]. The application of suitable preprocessing technique can improve the recognition rate in face recognition (FR) systems thereby increasing the accuracy to a greater degree. The noise and unwanted background details and be eliminated effectively in Edge Tracked Scale Normalization (ETSN) process which utilizes scale normalization technique with edge detection as a preprocessing technique.. But, the overall performance is not considerably high[4]. Another method based on chaotic encryption based blind digital image watermarking technique is suitable to both grayscale and color images. Here, Discrete Cosine Transform (DCT) is used prior to embedding process of watermarking in the host image [5]. A novel watermarking approach is employed for the embedding of a quantum watermark gray image into a quantum carrier image. The scrambled quantum watermark image by applying Arnold's cat map, is then incorporated into the quantum carrier image by concept of two least and most significant cubits[6].

IV. EXISTING SYSTEM

A. Figures and Tables

In existing systems, the watermarking is done by the steganography method is used to hide the data in an image by chaotic algorithm based on the mean and variance method. In this the data is sent to the receiver without encryption with the presence of third party in the channel. The content owner did not consider the presence of third party. In this the data is embedded in the form discrete statistics of histogram bins by the adjacent difference of the elements in the bins. It leads to small amount of distortion and provide modifications in the histogram shape. Mean and variance are calculated based on the vertex of radial co-ordinates in the spherical co-ordinates with the interval [0to1] and [-1to1] respectively. To avoid embedded distortion, the element transfer has been reduced by the histogram which takes large amount of time to transfer the data. The watermarking is done by pixel domain watermarking or by coefficient domain watermarking. DCT and DWT are done by coefficient domain watermarking for security issues. DCT is used in different frequency bands of the pixel for infinite sequence. By using DCT algorithm for data transmission it considers both low and high frequency of the pixel of an image but the data is embedded in the low frequency. Due to this reason it occupies more memory space. DCT is used for JPEG image compression and provide high computational cost. The DCT algorithm is used for quantum images using controlled NOT gate for encryption process. The data is watermarked by using NOT gate logic which provides less security, which cannot be used for long distance transmission. The data is arranged in the image's pixel in the form array segmentation.

V. PROPOSED SYSTEM

In this proposed method, the 3D .obj image is consider for watermarking by using slicing technique to embed the data into an image by DWT algorithm and by cryptographic method. The data are embedded in to a real time object image for data security. The 3D image undergoes vertical splicing to determine the frequency and energy of the image pixel. The frequency of the image pixel is separated as low frequency and high frequency pixel.

Retrieval Number: I8667078919/19©BEIESP
DOI: 10.35940/ijitee.I8667.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The data is transferred through low energy pixel to avoid the occupancy of large memory space. So, the low energy pixel is calculated from low frequency by using DWT algorithm. The data which is to be transmitted is in the binary form as ‘0’ and ‘1’. The bit is stored in the low energy pixel of an image. Then the image is reconstructed and transmission process takes place. The secret key is generated by using XOR gate between the data and the energy of the pixel. Then the key is transmitted between the sender and the receiver.

A. Methods Used

Slicing plays an important role in data compression with the maximum of 8bit. Each pixel is represented as 8bit as LSB and MSB bits. In this proposed system, vertical slicing is done to extract the vertex and faces of the image pixel to determine the frequency by DWT algorithm.

The preprocessing is done as histogram to determine the intensity of the pixel, which helps to reduce distortion during data transfer. The histogram equalization is to determine the dark and white patterns of the image pixel. Due to slicing technique, only dark pattern is present inside the image. So the histogram equalization is neutral.

Edge detection is done as canny edge detection which is more advantage than other edge detection for human visual perception. It helps to determine the appropriate image from the surrounding environment considering strong edge and weak edges and find the boundaries of the object of the image and helps to detect discontinuities in brightness. In 3D it helps to determine the volume of an image.

Data embedding is done in the form of bit in the image pixel with the resolution rate of 1:100.

The logical XOR operation is used to embed secret data in the image. It is performed between the energy of the pixel and data to be embedded to generate a secret key. The same process is repeated in the receiver side to determine the data from the image. Finally the MSE and PSNR value gets calculated.

B. Advantages

1.An attacker cannot reveal the original image content without secret key.
2.The Reconstructed image have the low MSE value.
3.This proposed scheme produces significantly lower complexity in computation than other existing schemes .

VI. EXPERIMENTAL RESULTS

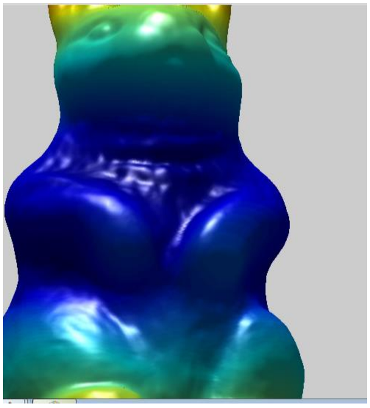


Fig.2.(i).3D .obj Image

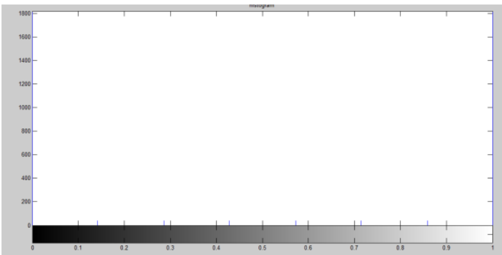


Fig.2.(ii).Histogram of obj Image

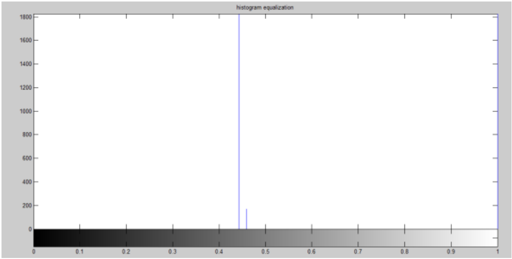


Fig.2.(iii).Histogram Equalization

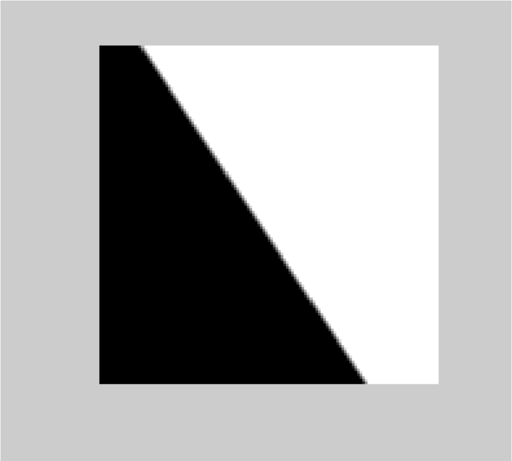


Fig.2.(iv).Image before Histogram Equalization

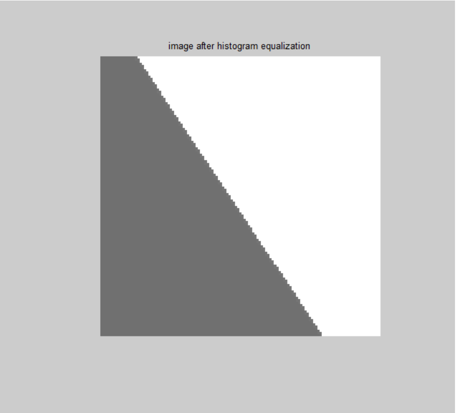


Fig.2.(v).Image After Histogram Equalization

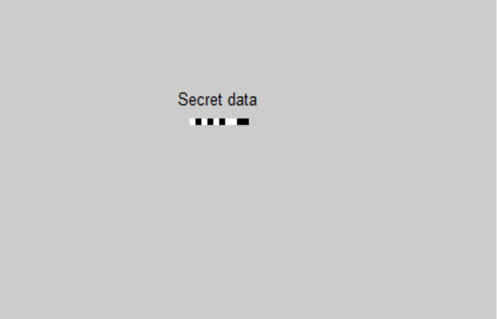


Fig.2.(vi) Secret Data

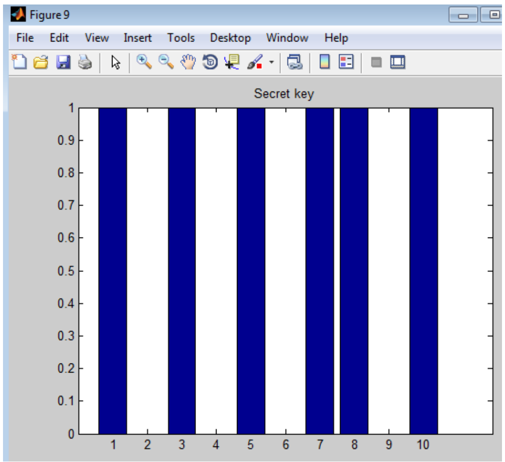
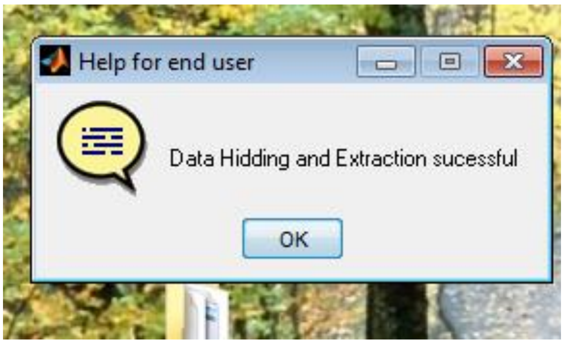


Fig.2.(vii) Secret Key Bar



Data Hidding and Extraction sucessful

Fig.2.(viii) Help for End user-Extraction Process

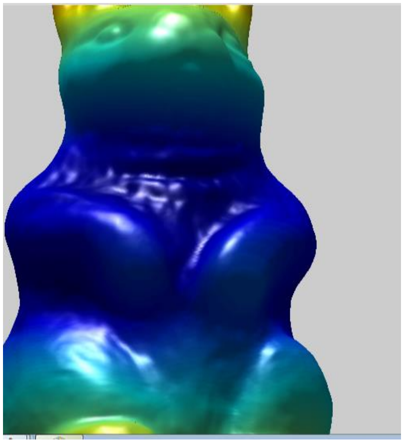


Fig.2.(ix).Reconstrucetd Image

VII. CONCLUSION

Security is very important during transmission in an allocated bandwidth.The security purpose is done by cryptographic method by the use of 'XOR' gate logic between energy pixel and the data. The pixel is as low energy pixel calculated by DWT algorithm. In this, the embedding and extraction of data into and from the image is achieved without any data loss and disortion.It provides low MSE value and high PSNR value.Hence the proposed system provides high embedding capacity than the other systems.

REFERENCES

1. Ying Yang, Ruggero Pintus, Holly Rushmeier, and Ioannis Ivrissimtzis, " A 3D Steganalytic Algorithm and Steganalysis-Resistant Watermarking" on IEEE TRANSACTIONS ON VISUALIZATION AND COMPUTER GRAPHICS, VOL. 23, NO. 2, FEBRUARY 2017
2. Nazir A. Loan1, (Student Member, IEEE), Nasir N. Hurrah1, (Student Member, IEEE), Shabir A. Parah1, (Student Member, IEEE), Jeon W. Lee2, (Member, IEEE), Javaid A. Sheikh1, (Student Member, IEEE), G. M. Bhat, " Secure and Robust Digital Image Watermarking using Coefficient Differencing and Chaotic Encryption" on DOI 10.1109/ACCESS. 2018.2808172, IEEE Access
3. Ahmed A. Abd El-Latif1, Bassem Abd-El-Atty1, M. Shamim Hossain 2,3, Senior Member, IEEE, Md. Abdur Rahman 4, Atif Alamri 2,3, B. B. Gupta 5 , " Efficient quantum information hiding for remote medical image sharing" on DOI 10.1109/ACCESS.2018.2820603, IEEE Access
4. S.V.V.D.Jagadeesh, T.Sudha Rani , "An Effective Approach Of Compressing Encrypted Images" on *IEEE Trans. Signal Processing*, 52(10), pp. 2992–3006,2007
5. "Smoothing And Optimal Compression of Encrypted Gray Scale Images" *IEEE Trans. Information Theory*, 52(4), pp. 1289–1306, 2008.
6. A.V. Sreedhanya and K.P. Soman, "Ensuring Security to theCompressed Sensing Data Using a Steganographic Approach" *IEEE Data Compression Conference (DCC '09)*, pp. 213–222, 2011.
7. Nitin Rawat, Pavel Ni, Rajesh Kumar, "A Fast Compressive Sensing Based Digital Image Encryption Technique using Structurally Random Matrices and Arnold Transform" *IEEE Trans. Information Forensics and Security*, 3(4), pp. 749–762, 2013
8. Amrita Sengupta, Sanjeev Ghosh, "Compression of Encrypted Images using Chaos Theory and SPIHT" *IEEE Trans. Signal Processing*, 19(4), pp. 1097–1102, 2016
9. Mr. Y. Sridhar, Mr. Bighneswar Panda, "Scalable Coding of PRNG Encrypted Images" IEEE 10th Workshop on Multimedia Signal Processing, pp. 760-764, 2016
10. M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.

AUTHORS PROFILE

J.Jansi Rani received the M.E. Degree from Sri Krishna College of Engineering and Technology affiliated to Anna University, TamilNadu,India in 2008. She is currently with the Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, TamilNadu, India. Her research interests include Digital Image Processing/ Denoising, Haze removal, Video signal Processing, and Optical Communication**.**

S.Anusuya received the M.E. Degree from Sri Krishna College of Engineering and Technology affiliated to Anna University, TamilNadu,India in 2019. She is currently with the Department of Electronics and Communication Engineering, Ramakrishna college of Engineering and technology, TamilNadu, India. Her research interests include Digital Image Processing Processing, Wireless sensor Networks

C.Senthamilarasi received the M.E. Degree from Sri Ramakrishna Engineering College affiliated to Anna University, Tamil Nadu, India in 2015. She is currently with the Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Tamil Nadu, India. Her research interests include VLSI design, Medical electronics, Digital low power circuit design.

Retrieval Number: I8667078919/19©BEIESP
DOI: 10.35940/ijitee.I8667.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)