LabVIEW based Multi-Image Encryption & Decryption Algorithm for Security & Data Authentication

Jayshree Verma[1] Dr. Monisha Sharma[2]
[1]M.Tech Scholar [2]Principal
[1,2]Department of Electronics & Telecommunication Engineering
[1,2]SSITM (Shri Shankracharya Technical Campus), Bhilai, India

Abstract— The sudden increase in encryption/decryption technology interest is most likely due to the increase in concern over copyright protection of multimedia content. With the rapid growth of the Internet and the multimedia image security systems in distributed environments encryption technique in multi images is a technique used to hide data or identifying information within the digital multimedia image. In the early days, encryption and decryption control access techniques were used to protect the image of media. Advance encryption algorithm technique becoming popular, especially for adding undetectable identification marks, such as copyright information. Because of this practical importance, watermarking techniques are often evaluated based on their invisibility, recoverability, and robustness. In this paper, the real-time image has been captured from the external device, in this work laptop from a camera (cam 0) has used for input of image to be encryption in interleave (JPG) format has taken, which is then converted into the number of frames. Each frame of the multi-image is then embedded with an algorithmic key using wavelet function. In this method, the level of WT can be easily controlled. Multi-resolution analysis has been performed on encrypted images and peak signal to noise ratio (PSNR) and mean square error (MSE) values have taken out to get the performance to differentiate between encrypted image and decryption image find out the accuracy and quality of image which actually depicts the efficiency and performance of AEC algorithm technique and the results of these has compared to one of the existing technique.

Key words: RT Image, Inverse Wavelets Transform. Labview, NI-Vision & Advanced Signal Processing Tools, IMAQ Vision

I. INTRODUCTION

We are living in the era of information where countless of bits of data is being created in each second and with the advent of internet, creation, and delivery of digital data (images, video and audio files, digital repositories and libraries, web publishing) has grown up. Since Xeroxing a digital data is very easy and fast too so, issues like, protection rights of the content and proving ownership, arises. Digital watermarking arises as a technique or tool to overcome shortcomings of current copyright laws for digital data sending and receiving end. The feature of advanced encryption standard algorithm is that it remains attached to the cover work even if it is copied and hacking of authenticated data. So to prove ownership or copyrights of data watermark is extracted and tested. It is very difficult for counterfeiters to remove or alter watermark. As such the real owner can always have his data safe and secure.

A. Real-Time Multi Image Capturing & Encryption & Decryption Technique

The boom in the information has its adverse effect too. Copying is nowadays simple with no loss of originality. A copy of a digital media is as same as to the original. This has in many instances, led to the use of digital content with malicious intent. There is a way to protect multimedia data against illegal retransmission and recording is to embed a signal, called digital signature or copyright or watermark that authenticates the owner. Due to the ability of editing and perfect reproduction in the digital domain, the protection of ownership and the prevention of unauthorized tampering of multimedia data have become important concerns. Data embedding has been gone through progress in recent years in both the academia and industry. Various techniques have been proposed for a variety of applications, including ownership protection, authentication, and access control. Imperceptibility, robustness against moderate processing such as compression, and the ability to hide many bits are the basic but rather conflicting requirements for many data hiding applications. In view of the above situation, propose to use the LabVIEW development platform to build the real-time multi-image copyright system based on a virtual instrument. The system used WT technology to design an effective algorithm, realizing the wavelength transformation embedded and blind extracted encryption. Solve the pirate tracing problem of multi-image copyright protection through embedding multiple encryption technique options and decryption wavelet Transform is recently adopted technology which is more advantageous than Fourier Transform (FT), Discrete Sine Transform (DST) and the Discrete Cosine Transform (DCT). Wavelet is an algorithm with the components like decomposition, thresholding, and reconstruction of the original image. There are tremendous applications in the area of image denoising which are used in scientific and engineering technology fields, medical science, Security and military services.

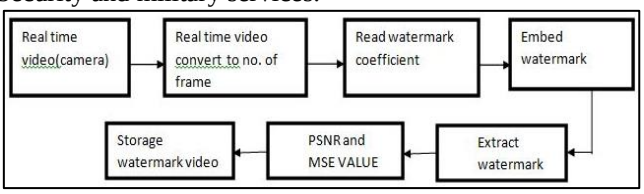

Fig. 1: Watermarking System

The Problem of illegal manipulation and distribution of multi-image encryption and a correct key to decryption information is becoming a big issue. To solve this problem, new technology has been proposed. Basically, it is a process of embedding copyright information into bit streams of any multi-images. In this particular scheme, the random segmentation and reconstruction of embedded secrete or encrypted data is done without knowing the original host

image. During the embedding process, secret data is embedded in the individual image matrix using the IMAQ toolbox of LabVIEW. In this proposed work, Integration and Encryption Algorithm technique has been introduced for authenticating data. We proposed a different type of wavelet-based digital Integration and Encryption Algorithm to secure data. In different wavelet, Dyadic equation is used to embed the copyright information in video bit streams.

The number of bits used to store the information of the image determines the resolution at intensity of the image A color mask is generally used (RGB Filter) for acquisition of color images. This filter allows decomposing the light in three bands, Red, Green and Blue. The three matrixes are generated and each one of them stores the light intensity of each RGB channel show to acquire video from a webcam using the NIVision Acquisition Express. This block is located in Vision/Vision Express toolbox and it is the easiest way to configure all the characteristics in the camera (cam0). Inside this block there are four sections: the first one corresponds to the option of select acquisition source which shows all the cameras connected in the computer. The next option is called select acquisition type which determines the mode to display the image and there are four modes: single acquisition with processing, continuous acquisition with inline processing, finite acquisition with inline processing, and finite acquisition with post processing. The third section corresponds to the configure acquisition settings which represents the size, brightness, contrast, gamma, saturation, etc. of the image and finally in the last option it is possible to select controls and indicators to control different parameters of the last section during the process. It was selected the continuous acquisition with inline processing, this option will display the acquired image in continuous mode until the user presses the stop button.

This chapter gives a brief introduction of digital encryption and decryption, its history, requirements, and application. Due to piracy of data they need to have some technique to prevent piracy and illegal copying of data arises. This need give rise to a new technique, known as Digital Watermarking. While proposing an algorithm some parameters are needed to keep in mind on which the proposed algorithm must be consistent. These parameters are discussed in the following section. Following sections are dedicated to watermarking application and attacks. A lot of work is going on for making watermarking techniques immune towards attack to retain the originality of image in receiving end and assuring successful extraction of encryption image to receiving the decryption image in receiving side with low error probabilities so to sort out disputes, if any, over copyrights or ownership of the image.

II. LITERATURE SURVEY

A.D.Senthil Kumar et al. proposed Multi Image Integration and Encryption Algorithm for Security Applications which is focused on implementing a secure image technique that enables to select one of the several images displayed simultaneously with a unique security key for each image. This process involves applying block based interleaving, followed by integrating the image matrix using the pixel-based integration technique and encrypting the images with Advanced Encryption Algorithm. With the key specifically generated for the image, the original image is decrypted from multiple images. Main object to find out is high entropy value and low correlation values provide good encryption and The time taken for encrypting and decrypting mosaic image with a key is 225.8394 seconds and for texture image is 228.0114 seconds to fast response of the system [1]

Balaji Tata, et al. proposed an Encryption and Decryption of Text File Using LabVIEW that is robust against video processing attacks. In this paper find out of efficient design is implemented to encrypt any text file and decrypt it using Fast Fourier Transform and Inverse Fast Fourier Transform algorithms respectively. The design is implemented in LabVIEW software. The basic operation in the encryptor module includes taking the input as the text file and converting the data into ASCII values and applying Fast Fourier Transform. To deny unauthorized access, a security key is added to the data and obtained output is copied into a file for transmission. In the decryptor module the received data is taken as input and decoded with the security key and Inverse Fast Fourier Transform is applied. The resultant ASCII values are converted into their corresponding string format. The text file that has to be encrypted is given as the input for the encryptor module. Encryption is performed using FFT algorithm and in order to provide security to our confidential data, a security key is added to it the received encrypted file is given as the input for decryptor module and the data is decoded using security key. Decryption is performed using the IFFT algorithm. The ASCII values are converted into its corresponding string format. [2]

Akansha Aswani et al. proposed a method for adding A LabVIEW Based Optimization of AES. Proposes a new method to combine Rijndael encryption and decryption algorithm implementation on LABVIEW with the strong focus on reducing area and high throughput. This AES algorithm implementation runs its symmetric cipher algorithm using encrypt /decrypt block and a key size of 256 bits. The proposed architecture implemented by LabVIEW. Which are synthesized map, place and routed using implementation on LABVIEW.AES is a symmetric encryption algorithm processing data in the block of 128 bits. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size.[3]

Phillip L. Reu, et al. proposed a Camera system resolution and its influence on digital image correlation. Digital image correlation (DIC) uses images from a camera and lens system to make quantitative measurements of the shape, displacement, and strain of test objects. This increasingly popular method has had little research on the influence of the imaging system resolution on the DIC results. This paper investigates the entire imaging system and studies how both the camera and lens resolution influence the DIC results as a function of the system Modulation Transfer Function (MTF).[4]

Mohit Kumar et al. proposed A Review on Various Digital Image Encryption Techniques and Security Criteria. The primary intention of keeping images protected is to maintain confidentiality, integrity, and authenticity. Different techniques are available for making images secure and one technique is encryption. Generally, Encryption is a procedure

that transforms an image into a cryptic image by using a key. Furthermore, a user can retrieve the initial image by applying a decryption method on the cipher image which is usually a reverse execution of the encryption process. For represents a primary image; a user operates an encryption technique and produces a secrete image Encrypted to histogram image and image encryption security parameters, permutation and substitution scrambling, and XOR operation.[5]

Kundan Kumar Rameshwar Saraf et al. proposed Text and Image Encryption Decryption Using Advanced Encryption Standard Due to an increasing use of computers, now day security of digital information is a most important issue. An intruder is an unwanted person who reads and changes the information while transmission occurs. This activity of intruder is called intrusion attack. To avoid such attack data may be encrypted to some formats that are unreadable by an unauthorized person. AES is mainly advance version of data encryption standard (DES). The input (block size Nb, also known as plaintext) of the AES algorithm is converted into a 4 x 4 array, called a state. Four transformations, AddRoundKey, SubBytes, ShiftRows, and MixColumns, perform various operations on the state to calculate the output state (the final cipher text). Except for AddRoundKey each of these operations is invertible. Inv Method (Method(a)) = a (2) If AddRoundKey operates on a variable twice, the variable itself is returned. [6]

K. Mohamed Hussain et al. proposed Anaglyph 3Dimesional Image Processing Using NI-LabVIEW 3Dimesional Imaging has become a highly emerging trend in recent times. But the conversion of 2Dimesional Images to 3Dimesional Images is not so easy and cannot be done at less cost. This paper deals with the conversion of 2D images into 3D with the help of NI-LabVIEW software. Two cameras which are mounted side by side serves as Left and Right eye to view the 3D image. Every Image has Red, Blue and Green components. By taking Red Component of Left image and Blue, Green Component of Right Image and merging these images will give you the Red-Cyan Image which is the traditional 3D image. The Extraction of Red, Blue, Green Component and Merging will be done through NI-LabVIEW. The Depth Image will be seen through a Red-Cyan 3D glass[7]

S helveen Pandey et al. proposed Best Symmetric Key Encryption-A Review. Advanced Encryption Standard is currently the best symmetric encryption algorithm for network security. AES specifies a fixed128-bit block size but different key lengths ranging from 128(10rounds), 192(12Rounds) and 256(14Rounds) bits (NIST, 2017). AES is block cipher algorithm. Many modern methods of symmetrick eyencryption utilize both stream and block schemes. An understanding of encryption can assist individuals in securing private data as well. With the evolution of Quantum computers, there is a risk to the encryption and suggestions mentioned is for Encryption security experts as well as Quantum developers to get together and get a solution to maintain security as security has been and will always be the main priority. [8]

Sudha Rani. K, et al. proposed" Text file encryption using FFT technique in Lab VIEW 8.6" In the proposed method, , The advantage of asymmetric over symmetric key encryption, where the same key is used to encrypt and decrypt a message, is that secure messages can be sent between two parties over a non-secure communication channel without initially sharing secret information. The disadvantages are that encryption and decryption are slow, and cipher text potentially may be hacked by a cryptographer given enough computing time and power. One very important feature of a good encryption scheme is the ability to specify a 'key' or 'password' of some kind, and have the encryption method alter itself such that each 'key' or 'password' produces a unique encrypted output, one that also requires a unique 'key' or 'password' to decrypt. This can either be a symmetric or asymmetric key[9]

Hiral Rathod, et al. Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm). An image based data requires more effort during encryption and decryption. The Proposed Architecture for encryption and decryption of an image using suitable user-defined key is developed with the same objective. In this paper, we introduce a new permutation technique based on the combination of image permutation and a newly developed encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". From the selected image we will binary value blocks, which will be rearranged into a permuted image using a permutation process, and then the generated image will be encrypted using.[10]

Krishan Gupta et al. Different image encryption and decryption technique and KA image cryptography. It additionally focuses on the functionality of Image encryption and decryption techniques and a KA encryption technique. KA Image cryptography is new approach in image cryptography which will be very helpful to improve image encryption. KA Technique Encrypt the image in two steps. First, apply different operation on image rows and column wise pixels. And then divide the whole image into Different parts and then apply different operation[11]

III. PROBLEM IDENTIFICATION

Digital image security has become highly important since the communication by transmitting digital products over the network occur very frequently. The image encryption algorithm is proposed, based on pixels interleaving with image integration. First, interleaving the image pixels, then through the method of pixel integration increasing the difficulty of decoding. At last, a different image for all the input images, getting the final encryption image. The experimental result shows good performance with low correlation and high entropy which shows that the pixel-based algorithm is highly secure. With this approach, it is also able to encrypt large volume of data more securely and the simultaneously new approach is expected to be useful for transmission applications and real-time system. The problem in includes the incorporation of other encryption algorithm and extending the images to videos. The AES architecture can be practically implemented successfully. Also, hardware implementation on LABVIEW carried out, verified encryption and decryption on the same device. As a result reduction of an area directly related to power consumption

The main strength of transform frequency domain techniques is addressing the restrictions of spatial methods,

moreover special features to represent an alternative view of a signal. The main drawback with frequency domain refers to high computational requirement but find out accuracy then wavelet technique based on a frequency domain.

IV. PROPOSED METHODOLOGY

The proposed methodology of this project based on IMAQ image processing tools and an advanced encryption standard algorithm based. Presented in this section is performed by a multi-image to pixel array conversion to find out the pixel value of each block. This conversion finds out Gaussian white noise, denoise using wavelet transform. Automatic histogram thresholding technique in its place of physically changing the threshold for the original image. The threshold selection is done automatically based upon the mean and standard deviation of each region among four sub-regions

A. Acquisition of Multi Images

Multi gray-scale is loaded to the algorithm and displays them with a different size example 200×200. A Gray-scale transformed image is well-defined by means of a huge matrix, its levels are numerical values between 0 and 255, black color represents the o level and 255 represent the white gray level. A digital grayscale image is nothing more than data—numbers indicating variations of black and white at a particular location on a grid of pixels. Most of the time, we view these pixels as miniature rectangles sandwiched together on a computer screen. With a little creative thinking and some lower level manipulation of pixels with code, however, we can display that information in a myriad of ways. This tutorial is dedicated to breaking out of simple shape drawing in Processing and using images (and their pixels) as the building blocks of Processing graphics.

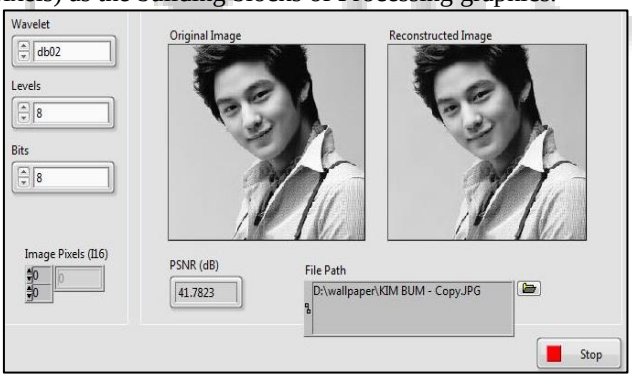

Fig. 2: Discrete Wavelet Transform (DWT) in Image Compression

B. Image Transformations

The images processing can be seen like a transformation of an image in another, in other words, it obtains a modified image starting from an input image, for improving human perception, or for extraction of information in computer vision. Two kinds of operations can be identified for them:

- Punctual operations. Where each pixel of the output image only depends on the value of a pixel in the input image.
- Grouped operations. In those that each pixel of the output image depends on multiple pixels in the input image, these operations can be local if they depend on the pixels that constitute its neighborhood, or global if they depend on the whole image or they are applied globally about the values of intensity of the original image.

C. Digital Image Acquisition

We generally associate the image to a representation that we make in our brain according to the light incidence into a scene (Bischof & Kropatsc, 2001). Therefore, there are different variables related to the formation of images, such as the light distribution in the scene. Since the image formation depends on the interaction of light with the object in the scene and the emitted energy from one or several light sources changes in its trip (Fig). That is why the Radiance is the light that travels in the space usually generated by different light sources, and the light that arrives at the object corresponds to the Irradiance. According to the law of energy conservation, a part of the radiant energy that arrives at the object is absorbed by this, other is refracted and another is reflected in form of radiosity.

D. Color Plane Extraction

In a 32-bit color image is coded in memory as moreover an RGB or an HSL image. RGB images quantity color data by means of 8 bits each for the red plane, green plane, and blue plane of color. In the HSL, color data is represented as 8 bits respectively for hue, saturation, and luminance, the alpha plane is used in both cases.

An array is a container object that holds a fixed number of values of a single type. The length of an array is established when the array is created. After creation, its length is fixed. The Image block displays the data in the array as an image. Each element of array specifies the color for 1 pixel of the image. The resulting image is an m-by-n grid of pixels where m is the number of columns and n is the number of rows. The row and column indices of the elements determine the centers of the corresponding pixels. The array values range from 0 to 255 to display the various shades of black.

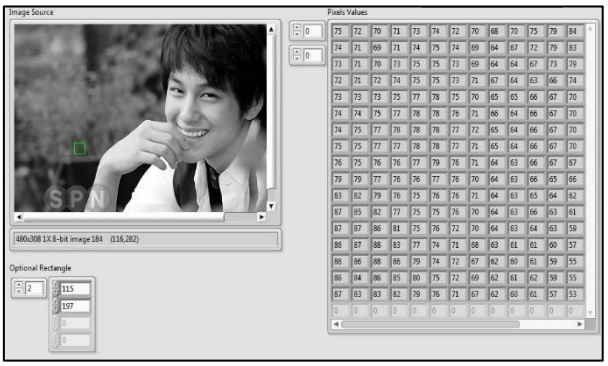

Fig. 3: Array of Pixel values from Image Parts

E. Histogram Analysis

Histogram of a digital image can be defined by frequency occurrence of pixels in a given image. In an 8-bit grayscale image 256 gray intensity shades are presented. For color images, three different histograms of Red, Green, Blue can also be developed.

It is evident from the statistics of four histograms that the mean value in the right half and lower half are greater than 50 where maximum values are 255. The average standard deviation from the mean value is also high in these regions. By this, it is assumed that the tumor lies in the

regions as there are more high-intensity pixels. The histogram is a graph that contains the number of pixels in an image at different intensity value. In an 8-bit greyscale image, a histogram will graphically display 256 numbers showing the distribution of pixels versus the grayscale values as is shown in Fig.

Fig. and Fig. shows the results of the grayscale histogram and RGB histogram using IMAQ histogram block located in Image Processing/Analysis. The output of the IMAQRead Image Block is connected to the input of the IMAQ histogram block and then a waveform graph is connected in order to show the obtained results.

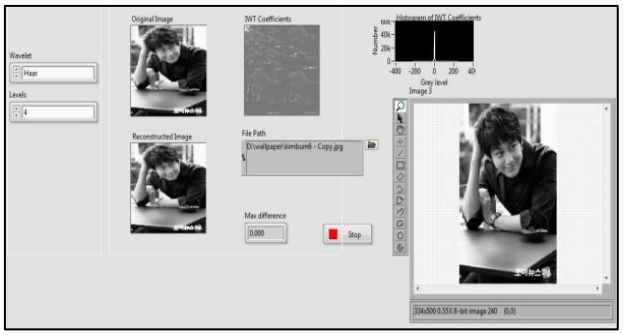

Fig. 4: Histogram Analysis of Image difference between the Original and the Reconstructed Image

F. Threshold Selection

1) Step 1: Calculate avg. std. variation for 4 regions.
2) Step 2: calculate sum= Σ mean of no mask regions.

In the proposed thresholding technique, a predefined value is compared to the standard deviation of each region. Based on this result image masking is performed. After the masking operation is completed threshold value is selected by adding the means of all the regions.

Fig. 5: Wavelet Transforms in Detecting Image

V. RESULT

The proposed algorithm in this paper is applied to a sample image and real-time capture image which has been taken from laptop front camera itself in jpg format. The proposed algorithm shows good image encryption ability since the original sample frame and its corresponding encryption and decryption frame looks quite identical. The performance of the proposed algorithm is used to hiding/encrypted the defense data with high security. It is tested using real-time image (jpg). The size of the frame is 640x480. This algorithm is evaluated when varying the size of the image by changing the different level and wavelet function in the embedded secret key.

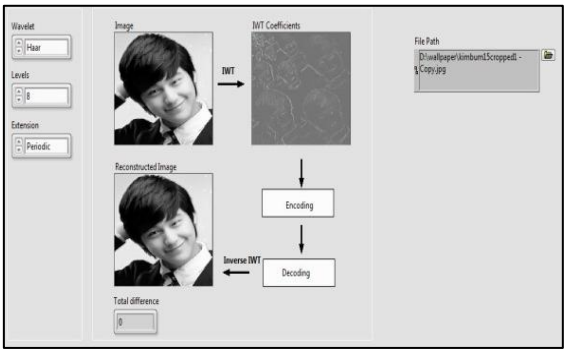

Fig. 6: WT Tech. Encoding and Decoding of Image

In the current works implementation of digital multi-image encryption technique based on Wavelet Transform (WT) is proposed. DWT technique is robust among all due to its multi-resolution capability. Graphical programming is created using LabVIEW. In this proposed technique encrypted secret key frames are almost identical to original image frame decryption for low values of embedding strength. The proposed technique is less time consuming since it does not require tedious programming.

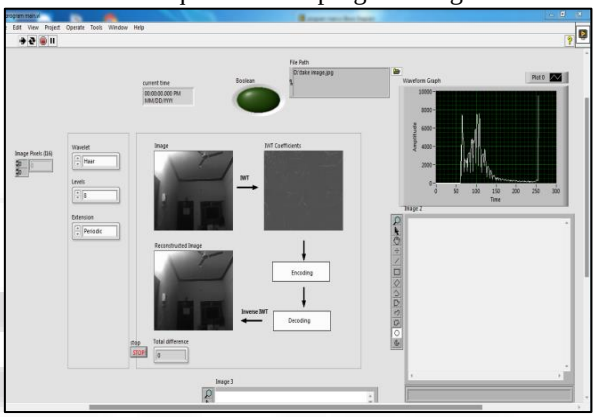

Fig. 7: Labview Program Front Panel (GUI) Using Real Image Capturing

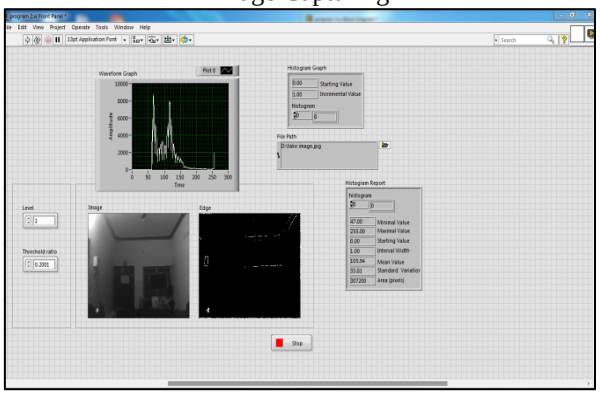

Fig. 8: Labview Program Front Panel (GUI) for Thresholding Value

A. Comparision of the Proposed Method with Earlier Work

Although this project is primarily focused on multi-image encryption and decryption of real-time capture image using Labview and IMAQ toolbox using DWT technique, and the results of the same have already been discussed earlier. However to compare the accuracy of the proposed method the same input has to be given as discussed in the work done by A.D.Senthil Kumar and T.S.Anandhi [1]. To compare the result a High entropy value and low correlation values

provides good encryption. The time taken for encrypting and decrypting mosaic image with a key is 225.8394 seconds and for texture image is 228.0114 seconds.

SN	Property	particular
1	Resolution	640x480
2	time	105.8548 sec.

Table 1: Properties of Input Video Taken for Comparison

From the above results, it can be found that the proposed method of multi-image encryption as performed well as compare to propose in [1]. The encryption time has taken for comparison and it has been found that time taken value is lesser in this proposed method.

B. Conclusion

In the current work implementation of digital multi image encryption technique based on Wavelet Transform (WT) is proposed. DWT technique is a robust among all due to its multi resolution capability. Graphical programming are created using LabVIEW. In this proposed technique encrypted secret key frames are almost identical to original image frame decryption for low values of embedding strength. The proposed technique is less time consuming since it does not required tedious programming.

C. Future scope

For the future work various attacks can be applied in this proposed model and their effect on image encryption and decryption can be studied also this model can be compared with other multi image encryption in frequency domains DCT, DFT etc.

REFERENCES

[1] A.D.Senthil Kumar, T.S.Anandhi, " Multi-Image Integration and Encryption Algorithm for Security Applications ", 978-1-5090-3474-1/16 IEEE Communications, 2016.

[2] Balaji Tata, Surya Prasada Rao Borra, Geetha Devi Appari, "Encryption And Decryption Of Text File Using LabVIEW", IJRECE VOL. 6 ISSUE 3 (JULY - SEPTEMBER 2018), ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).

[3] Akansha Aswani 1, Prof. Sachin Malviya 2, "A LabVIEW Based Optimization of AES", International Journal of Innovative Research in Computer and Communication Engineering Vol. 5, Issue 10, October 2017, ISSN (Online): 2320-9801 ISSN (Print): 2320-9798.

[4] K. Sudharani1*, T. C. Sarma2 and K. Satya Prasad3," Histogram Related Threshold Technique for Region-based Automatic Brain Tumor Detection", Indian Journal of Science and Technology, Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/89891, December 2016, ISSN (Print): 0974-6846 ISSN (Online): 0974-5645.

[5] Mohammed Abo-Zahhad, Sabah M. Ahmed, and Ahmed Zakaria, "An Efficient Technique for Compressing ECG Signals Using QRS Detection, Estimation, and 2D DWT Coefficients Thresholding", Hindawi Publishing Corporation Modelling and Simulation in Engineering Volume 2012, Article ID 742786, 10 pages doi:10.1155/2012/742786..

[6] Phillip L. Reu, William Sweatt, Timothy Miller, and Darryn Fleming, "Camera system resolution and its influence on digital image correlation" SAND2013-8737J.

[7] Mohit Kumar, Akshat Aggarwal, Ankit Garg "A Review on Various Digital Image Encryption Techniques and Security Criteria", International Journal of Computer Applications (0975 – 8887) Volume 96– No.13, June 2014.

[8] Kruti Goyal, Hadi Baghsiahi & David R Selviah "Automatic Segmented Area Structured Lighting", Proceedings of the 17th Irish Machine Vision and Image Processing conference IMVIP 2015, August 26th-28th, 2015, Dublin, Ireland, ISBN 978-0-9934207-0-2.

[9] Kundankumar Rameshwar Saraf1 , Vishal Prakash Jagtap2 , Amit Kumar Mishra3 "Text and Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May – June 2014 ISSN 2278-6856.

[10] K. Mohamed Hussain, R. Allwyn Rajendran Zepherin, S. Abirami "Anaglyph 3Dimesional Image Processing Using NI-LabVIEW", IJIRST –International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 8 | January 2015 ISSN (online): 2349-6010

[11] Shelveen Pandey, Mohammed Farik "Best Symmetric Key Encryption - A Review", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 6, ISSUE 06, JUNE 2017, ISSN 2277-8616

[12] Sudha Rani. K 1 , T. C. Sarma 2 , K. Satya Prasad3 "TEXT FILE ENCRYPTION USING FFT TECHNIQUE IN Lab VIEW 8.6", IJRET: International Journal of Research in Engineering and Technology, ISSN: 2319-1163 .

[13] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3.

[14] KRISHAN GUPTA "DIFFERENT IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES AND KA IMAGE CRYPTOGRAPHY"International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-1, Issue-10, Dec-2013.

[15] Kaladharan N "Unique Key Using Encryption and Decryption of Image" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10, October 2014, ISSN (Online) : 2278-1021 ISSN (Print) : 2319-5940

[16] Prerna#1 , Urooj#2, Meena kumari#3, Jitendra Nath shrivastava#4 "Image Encryption and Decryption using Modified Hill Cipher Technique", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1895-1901.

[17] www.ni.com\manual

