International Journal of Engineering Science Invention Research & Development; Vol. I Issue II August 2014
www.ijesird.com e-ISSN: 2349-6185

A Novel Approach for Proactive Wireless Data Transmission

Ms. Chaitali R. Bagul[#], Kokate M. D.[*]
[#*]*E&TC Dept, KKWIEER, Panchavti, Nasik, India*
[#]chaitali.bagul7@gmail.com,*mdkokate@rediffmail.com

***Abstract*—Security is one of the important aspects in computer communication. System is based on novel approach for transmission of data with concealed information is evinced. In this approach, we convert gray image into RGB, the RGB image is then compressed with the help of DCT. Compressed image is then watermark, and the secure information is concealed. At the last we encrypt the image using encryption algorithm to transmit over channels wirelessly. Frequency and Spatial domain transformation tools have been used to achieve security. The information is embedded as watermark into the lower order bits of the image pixels. To enhance the robustness of the embedded Information, the encrypted watermark is compressed by using wavelets.**

At the receiver end, the received image is decrypted first to uncompress. The image is extracted; watermark accuracy depends on the region of the image into which it is embedded. Hence extracted watermark accuracy is evaluated for three different regions of the image with no noise. The bursty wireless channel is simulated by adding impulse noise to the embedded image. Extracted image is uncompressed using IDCT and converted into gray image. The efficiency of the proposed approach is illustrated with the implementation results on an encrypted and decrypted image.

***Keywords*— Image Encryption, Encryption, Decryption, Advance Encryption Standard (AES), Discrete Wavelet Transform (DWT), Image Quality.**

I. INTRODUCTION

Now days in an entire range of everyday life digital media is stored efficiently and with a very high quality but by using computer systems it can be manipulated very easily. Also digital data can also be transmitted through data communication networks without losing quality in a fast and inexpensive way. With digital multimedia, distribution over World Wide Web (WWW) Intellectual Property Right (IPR) is more threatened
than ever due to the possibility of unlimited copying. So by using some encryption techniques the easily copying of the data need to be restricted. Once the encrypted data are decrypted, it can be freely distributed or manipulated.

This problem can be solved by hiding some ownership data into the multimedia data which can be extracted later to prove the ownership. Data transfer is transferring information from a location or host to another host, or server. To have a secure data transfer, few method can be applied, and one of them is encryption of data, prepare it to be transferred in encrypted way and decrypted when the data want to be used.

II. METHODOLOGY

The project is divided into four segments like Gray to Color image conversion, Image compression, Digital watermarking image, Image Encryption.

Here we introduce new method in which a general technique for ”colorizing” grayscale images by transferring color between a source (color image) and a destination (grayscale image). Rather than choosing RGB colors from a palette to color individual components, we transfer the entire color ”mood” of the source to the target image by matching luminance and texture information between the images. We choose to transfer only chromatic information and retain the original luminance values of the target [1].

Image Compression addresses the problem of reducing the amount of data required to represent the digital image. Compression is achieved by the removal of one or more of three basic data redundancies:

- Coding redundancy, which is present when less than optimal code words are used.
- Interpixel redundancy, which results from correlations between the pixels of an image.
- Psycho visual redundancy which is due to data that is ignored by the human visual system.

In Digital Watermarking awe embedding a hidden stream of bits in a file is done. The file could be an image or text. Nowadays, digital watermarking has many applications such as broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control and file reconstruction. Image Encryption techniques try to convert original image to cipher image that is hard to understand and to keep the image confidential between users [2]. This image contains various different properties: high redundancy and high correlation among adjacent pixels that demands special encryption algorithm for images.

For the efficient transmission of an image across a channel, source coding in the form of image compression at the transmitter side and the image recovery at the receiver side are the integral process involved in any digital communication system. Other processes like channel encoding, signal modulation at the transmitter side and their corresponding inverse processes at the receiver side along with the channel equalization help greatly in minimizing the bit error rate due

to the effect of noise and bandwidth limitations (or the channel capacity) of the channel.

Following figure shows the block diagram of purposed system.

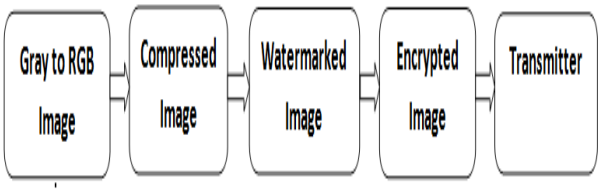

Fig. 1 Transmitter Side

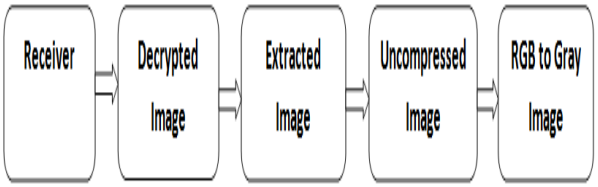

Fig.2 Receiver Side

A. Gray to Color Image Conversion

Here, the algorithm for transferring color is described. First each image is converted into the color space. We use jittered samplings select a small subset of pixels in the color image as samples.

Both color (source) and grayscale (target) images are converted to the décor related space for subsequent analysis. Space was developed to minimize correlation between the three coordinate axes of the color space. Thus, changes made in one

Color channel should minimally affect values in the other channels. The color space is selected because it provides a decor related achromatic channel for color images. It allows us to selectively transfer the chromatic channels from the color image to the grayscale image without cross-channel artifacts. In order to transfer chromaticity values from the source to the target, each pixel in the grayscale image must be matched to a pixel in the color image. The comparison is based on the luminance value and neighborhood statistics of that pixel [1]. The neighborhood statistics are recomputed over the image and consist of the standard deviation of the luminance values of the pixel neighborhood. It allows us to reduce the number of comparisons made for each pixel in the grayscale image and decrease computation time. Once the best matching

Pixel is found, the chromaticity values are transferred to the target pixel while the original luminance value is retained. Algorithm for color conversion is as follows

i. Read color Image (source).
ii. Read grayscale Image (target).
iii. Convert source image and target image into binary.
iv. Compare Pixels of color (source) & grayscale (target) with each other.
v. Both converted to the decor related space.
vi. If pixel match then go next, else go back to stage.
vii. Transfer the chromatic channels from the color image to the grayscale image without cross-channel artifacts.

B. Image Compression

Image compression is a technique to reduce the storage and transmission costs. The discrete cosine transform (DCT) helps to separate the image into parts of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.

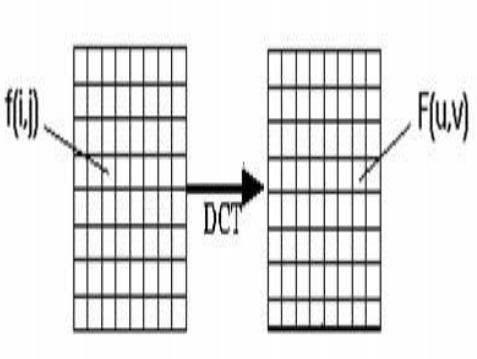

Fig. 3 Transformation of function into DCT

DCT expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG), to spectral for the numerical solution of partial differential equations.

For compression, cosine functions are more efficient and for differential equations, it expresses particular choice of boundary conditions. DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT). Algorithm for image compression

i. Read image generated from the compression
ii. Perform image segmentation, divide source image into 8x8 Blocks.
iii. After this, apply DCT on image.
iv. Quantization on image.

v. Encode and reconstruct the image.
vi. Compressed image is obtained.

C. Watermarking Image

Watermarking techniques are classified into two categories: such as spatial domain methods and transform domain methods. Spatial domain methods are less complex as no transform is used, but are not robust against attacks. Transform domain watermarking techniques are more robust in comparison to spatial domain methods [5]. As when image is inverse wavelet transformed watermark is distributed irregularly over the image, making the attacker difficult to read or modify. Watermarking using discrete wavelet transform (DWT) are gaining more popularity as it has a number of advantages such as progressive and low bit-rate transmission, quality scalability and region-of-interest (ROI) coding demand more efficient and versatile image. The basic idea of DWT in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency band. Then transforms the coefficient of sub-image. After the original image has been transformed into DWT, it is decomposed into 4 frequency bands, one is low frequency band (LL) and three high frequency band (LH, HL, HH) [6].

Algorithm for Watermarked Image

i. First read the image generated from compression algorithm.
ii. Perform DWT on first Image, to find out coefficient.
iii. Select Particular coefficients.
iv. Read Second Image.
v. Apply DWT on second image.
vi. Embedded second image into first image for watermarking.

Algorithm for Watermarked Extraction

i. First read Watermarked Image.
ii. Perform IDWT on Watermarked Image, to find out coefficient.
iii. Select particular coefficients.
iv. Extract original Image.
v. Apply IDWT on second image.
vi. Read Original Image.

D. Image Encryption and Decryption

Image encryption has been increasingly studied to meet the demand for real-time secure transmission over the internet and through wireless networks. The combination of chaotic theory and cryptography forms with numerical key is an important field of information security. Due to some inherent features of images like bulk data capacity and high data redundancy, the encryption of images is different from that of texts; therefore it is difficult to handle by traditional encryption methods. In this communication, new image encryption algorithms based on three different methods are proposed. In encryption we combine three different algorithms to generate an image like AES, DWT, Huffman coding. In this method, AES algorithm is used for encryption. DWT and Huffman coding is used to manipulate the pixel used in AES encryption.

AES Algorithm

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001 [7]. Based on the Rijndael cipher Joan Daemen and Vincent Rijmen, submitted a proposal which was evaluated by the NIST during the AES selection process [8]. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. AES operates on a 44 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. AES algorithm is governed by four transformations like Add round key, Sub Byte transformation, Shift Row Transformation, Mix Column Transformation.

DWT Algorithm

Most watermarking techniques transform the host image into a domain that facilitates embedding of the watermark information in a robust and imperceptible way. Wavelets are functions that satisfy certain mathematical requirements and are used in representing data or other. Wavelet algorithms process data at different scales and resolutions. Wavelet transform uses wavelets as basis and is a tool that cuts up data or functions or operation into different frequency components, and then studies each component with a resolution matched to its scale. The original image is decomposed by the low pass (LP) and high pass (HP) filters followed by down sampling first of rows and then of columns. The result of wavelet decomposition is approximation of original image and three detail signals (horizontal, vertical and diagonal).

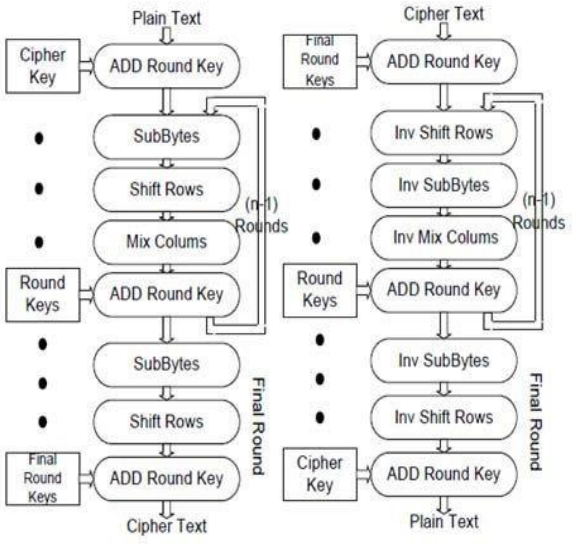

Fig. 4 Design flow of AES algorithm

Huffman Coding Algorithm

A Huffman code is an optimal prefix code in computer science and information theory found using the algorithm developed by David A. The process of finding or using a code is called Huffman coding and is a common technique in entropy encoding and in lossless data compression. The algorithm's output can be viewed as a variable-length code table 26 for encoding a source symbol [9]. Huffman's algorithm derives the table based on the estimated probability or frequency of occurrence (weight) for each possible value of the source symbol. As in other entropy encoding methods, more common symbols are generally represented using fewer bits than less common symbols. Huffman's method can be efficiently implemented, finding a code in linear time to the number of input weights if these weights are sorted.

Huffman coding uses a specific method for choosing the representation for each symbol, resulting in a prefix code.

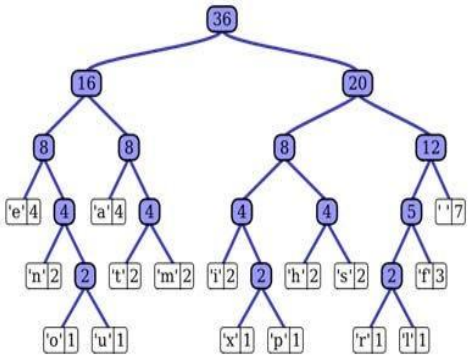

Fig. 5 Huffman Tree

Algorithm for Encryption and Decryption is as follows

i. First read Watermarked Image.
ii. Perform DWT on Watermarked Image and quantization of image.
iii. Perform AES algorithm and compress bits using Huffman coding.
iv. Encrypt and encode the data.
v. Apply Huffman decoding and AES decryption.
vi. Inverse Quantization and inverse DWT on image
vii. Decrypted image is obtained.

III. COMMUNICATION VIA BLUETOOTH

In this project, communication or data transfer takes place Bluetooth. Wireless 1704 Bluetooth v4.0 + hs is used. Bluetooth is managed by the Bluetooth Special Interest Group (SIG), in the areas of telecommunication, computing, networking, and consumer electronics. Bluetooth was standardized as IEEE 802.15.1, but the standard is no longer maintained. It is a wireless technology standard for exchanging data over short distances (using short wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz)from fixed and mobile devices, and building personal area networks (PANs). It can connect several devices, overcoming problems of synchronization.

Fig. 6 Bluetooth 4.0

Features of Bluetooth v4.0 + hs

i. Range is up to 300 feet or more.
ii. Bluetooth 4.0 adapts low-energy specification (BLE).
iii. Reliable point-to-multipoint data transfer with advanced power-save and secure encrypted connections at the lowest possible cost.
iv. t consumes Low Power or Low Energy.
v. It uses 2.4 GHz radio frequencies which allow dual-mode devices to share a single radio antenna.
vi. Peak current consumption is < 15mA.
vii. Over the air data rate is 1 Mbit/s.
viii. Application throughput 0.27 Mbit/s.
ix. Bluetooth v4.0 has 40 2-MHz channels.
x. It uses frequency hopping to counteract narrowband interference problems.

IV. RESULTS AND ANALYSIS

In this chapter, the experimental results are shown according to the steps mentioned in methodology. The output of each step after its execution is shown using images.

Complete system is implemented in Graphics User Interface (GUI). Each module is executed according to the sequence.

A. *Transmitter Side*

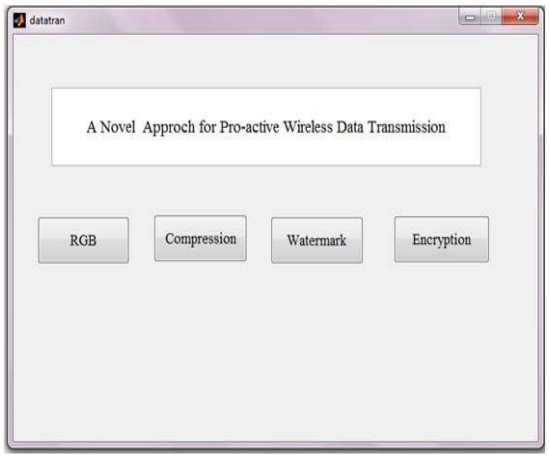

Fig. 7 Transmitter Side GUI Panel

Step 1: Gray scale to color image conversion.

Firstly, from the GUI panel we click on RGB Block to convert the grayscale image to color image. Obtained image is resultant color image.

Fig. 8 Gray Scale Image

Fig. 9 Reference Color Image

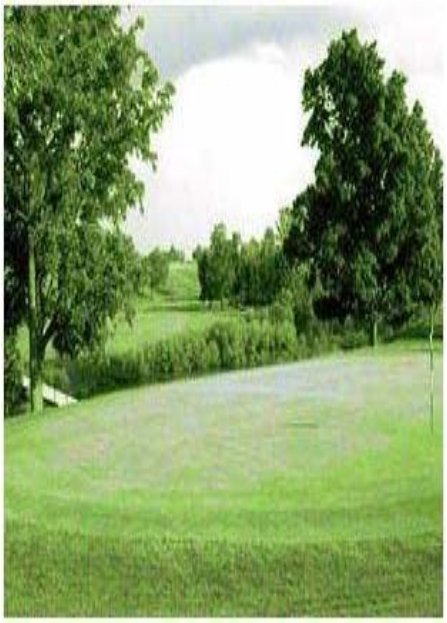

Fig. 10 Output Color Image

Step 2: Image compression:

Here, we compress image generated in first step, i.e. ColorImage.jpg. Here actual Size of image ColorImage.jpg is 23.3 kb. After Compression, size gets reduced to 16.1 Kb. Image obtained after compression is called a compressed image.

Fig. 11 Compressed Image

Step 3: Watermarking.

By using watermarking we embedded the data image which is to be transmitted over wireless network by using the DWT algorithm.

First, select Host Image: Original new image.

Select Watermark Image: Compressed image as shown in fig.11

Here, compressed image is to be hiding behind original image. While simulating the watermarking, we obtained the DWT's of the original image and also resultant watermarked image.

Fig. 12 Original new Image

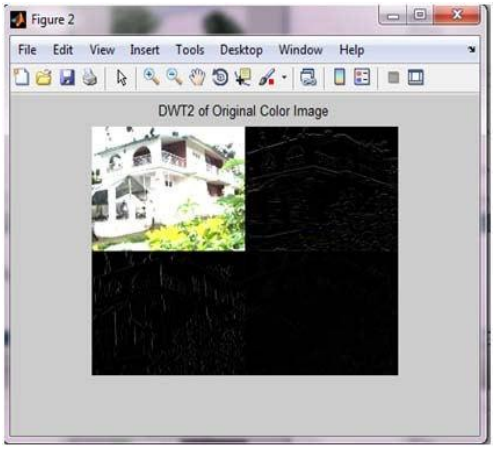

Fig. 13 DWT of original new image

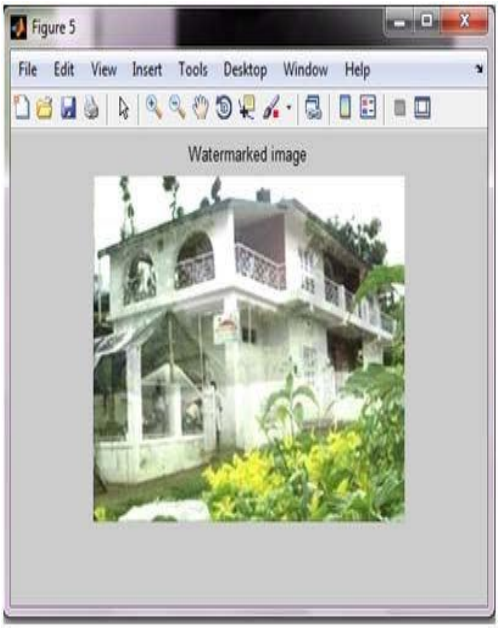

Fig. 14 Watermarked Image

Step 4: Encryption

Obtained Watermarked image is encrypted using the AES, DWT and Huffman Coding. Huffman and DWT perform pixels manipulation on the image. Also Key is used for secures data transfer. For executing of encryption code we have to press on push button of Encryption as shown in fig. 15.

Following window is obtained by clicking on the encryption button. Source image is considered along with key and image data which is to be send, is encrypted with source image. We use key '2'. In this window we put full path of source image along with key, path where output image is saved and data image which is to be transfer.

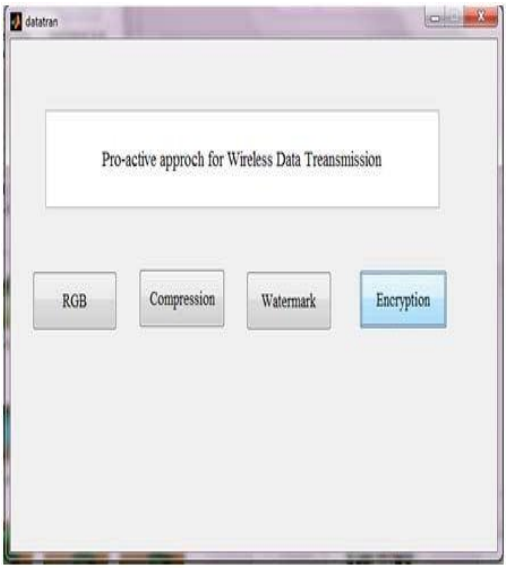

Fig. 15 Window for Encryption

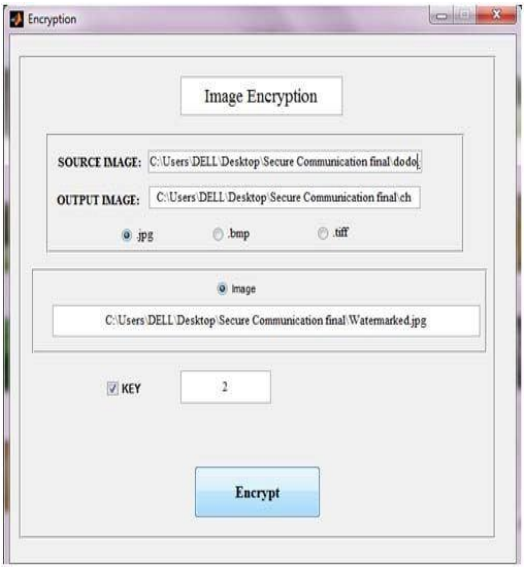

Fig. 16 Encryption Panel

Fig. 17 Source Image, Data Image and Encrypted Image

B. *Receiver Side*

Inverse of the encryption (Decryption process) is performed at the receiver side. Here Output image generated in Encryption part is decrypted to recover original image. By calling the decryption code following window is open.

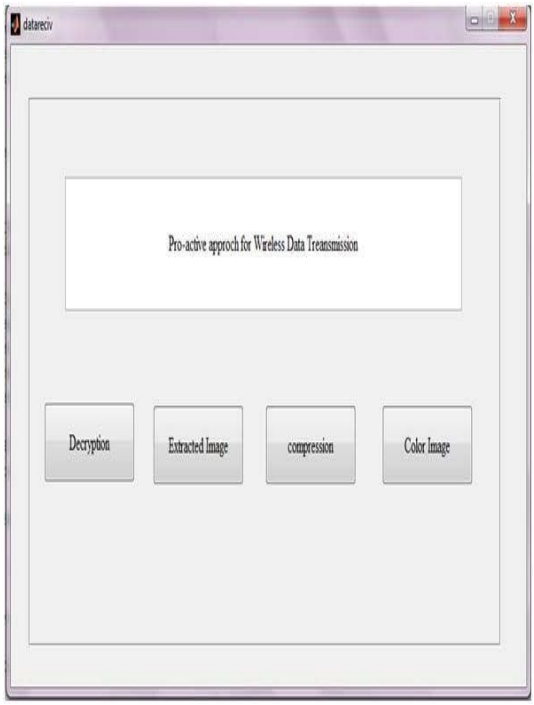

Fig. 18 Receiver Side GUI panel

By clicking on the decryption, following window for the decryption is obtained. And by placing the path of encrypted image and putting key '2' same as that of encryption, decrypted image is obtained. Obtained decrypted image is extracted from original image by using IDWT and later extracted image is converted to grayscale image to obtain the original image.

Fig. 19 Window for Decryption

Fig. 20 Decrypted Image

Thus, Experimental results are tested and evaluated on Matlab2012a. Performance is tested and evaluated on Intel(R) Core(TM) i3-3217U CPC @ 1.80 GHz 64 bit system with 4 GB RAM running Windows 7 Professional.

Fig. 21 Extracted Image

Fig. 22 Original grayscale Image

Conversion of gray to color image algorithm works well on scenes and landscape, image is divided into distinct luminance clusters or textures. It takes time ranging from few sec to hundreds of sec depending on the pixels range, By using, texture classification method, more images can be colorized. Results of watermarking are effective as the watermarked image looks almost same as that of the original image. All kind of attacks are refused by the good encryption system. Security analysis is performed and various quality measured parameters is obtained from the implemented algorithm.

C .Graphical Representation

Figure obtained below shows the graph of size for encrypted and decrypted image with original image. From the result, it clearly shows that the both the images obtained are similar as their graph are linearly same,

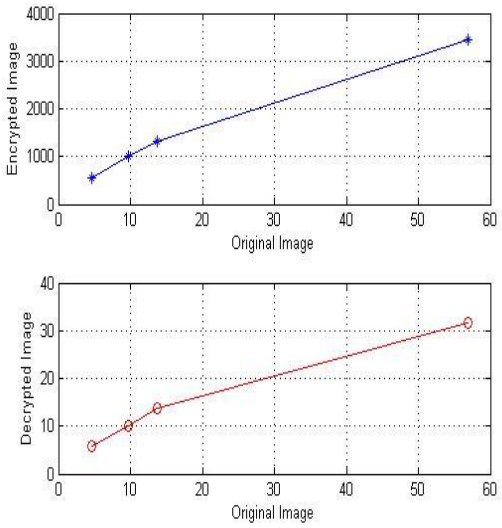

Fig. 23 Graph of Original Image with Encrypted Image and Decrypted Image

Peak Signal to Noise Ratio (PSNR), is an engineering term for the ratio between maximum possible power of signal and the power of corrupting noise that affects the fidelity of it representation. PSNR is mostly used as measure of quality of reconstruction of an image. Here, signal is the original image and noise is the distortion introduced by encryption. High PSNR indicates reconstruction is of high quality.

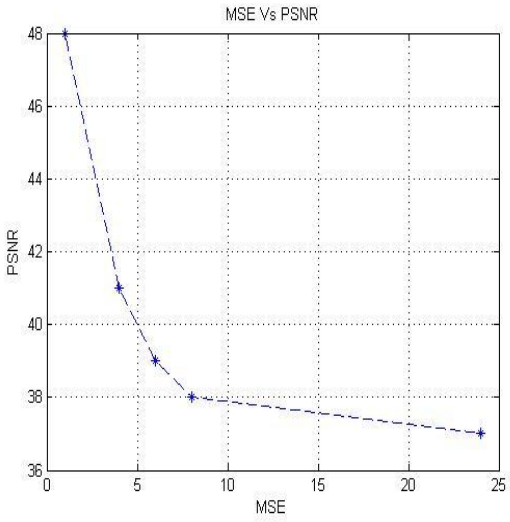

Fig. 24 Graph of MSE Vs PSNR

D Image Quality Measures

By the implemented algorithm, various image quality parameters of the encrypted image is evaluated and represented in tabular form.

TABLE I
IMAGE QUALITY MEASURES FOR ORIGINAL AND ENCRYPTED IMAGE

Image Size	MSE	PSNR	Encryption Time (sec)	Decryption Time (sec)
5KB	1.0017	48.123	0.677	0.0009
10KB	4.2107	41.88	0.3500	0.0014
12.8KB	6.27	40.158	0.9600	0.0019
13.7KB	8.945	38.614	0.3548	0.0020
55KB	22.3415	34.63	0.8943	0.0019

V. CONCLUSION

Thus we developed a user friendly, general and new approach to transfer data from one side to another. We are

successful in implementing the algorithm that transfers important data by embedding in another image by giving high level security. AES and Huffman algorithm plays important role for pixels manipulation of images. Also, Graphical results shows our system is good as PSNR increases. Various image quality parameters are calculated, which signifies less noise is introduced while transferring data. Normalized Cross correlation is found to be 0.99 and structural content obtained is 1 of Original and Encrypted Image. Future work may involve combining implemented algorithm with some new technique in order to accomplish data hiding and to provide more security against various known attacks.

ACKNOWLEDGMENT

I owe my deepest gratitude and indebtedness to my highly respected and esteemed guide Prof. M. D. Kokate, Department of Electronics & Communication Engineering, K. K. Wagh engineering College, Nasik (Maharashtra) for being a continuous source of inspiration and guidance, sincere criticism and regular feedback on my advancement each week I was able to learn and improve upon our working strategy and thus, enhance our approach during this piece of work. It was because of his stimulating suggestions and comments that I could identify the right topic and always keep in the right track. I would like this opportunity to express my sincere thankfulness to HOD of Electronics& Communication Department for his encouragement, inspiration and kind approval of this project. I think him for providing the required resources from the college. I am equally indebted to the supporting staff members of Dept. of E&T/C, KKWIEER, and Nasik who have helped me directly or indirectly.

REFERENCES

[1] Govind Haldankar, Atul Tikare, JayprabhaPatil, "Converting Gray-Scale mage to Color Image", *Proceedings of SPIT-IEEE Colloquim*, Vol.1, pp.189-192, 1998.

[2] Samir Kumar Bandyopadhya, Tuhin Utsab Paul, Avishek Ray choudhary,"ImageCompressionusingApproximationMatchingandRunLength",*International Journal of Advanced Computer Science and Application(IJACSA)*,Vol.2,No.6,2011.

[3] Chaitali R.Bagul, Kokate M.D. "Image Colorization: Transformation to luminance to chrominance with matching approach", *International Journal of Elsevier Science and Technology*, July2014.

[4] R.C.Gonzalez, R.E.Woods, S.L.Eddins, Digital *image processing using MATLAB*, McGrawHill, 2011.

[5] BhupendraRam,"Digital Image Watermarking Technique using Discrete Wavelet Transform and Discrete Cosine transform", *International Journal of Advancement in Research & Technology"* ,ISSN:2278-7763,Vol.2,Issued4,April2013.

[6] S.Kother Mohideen, Dr.S.Arumuga Perumal, Dr.M.Mohamad Sathik, "Image Denoisingusing Discrete Wavelet Transform", *InternationalJournalofComputerScienceandNetworkSecurity (IJCSNS)*, Vol.8No.1, pp.213-216, January2008.

[7] Federal Information Processing Standards Publication197 (FIPS197), "http://csrc.nist.gov/publications/fips/fips197/fips-197.pdfS, 2001."

[8] J.Daemen,V.Rijmen,"TheblockcipherRijndael",*InternationalJournalofSmartCardResearchandApplications*,pp.288-296,2000.

[9] J.JaspalKaurSaini,KritiSaini,"NewAdvanceEncryptionStandardtoAnalyseEncryptedImageQuality",*International Journal of compute r Application*, ISSN:0975-8887,Vol.74No.7,July2013