Novel Image Digital Rights Management Scheme

[1]Honey Mary Baby, [2]Kuttyamma A.J
[1]Student, [2]Professor(HOD)
[1]Information Technology,
[1]Rajagiri School of Engineering and Technology, Kerala, India

Abstract : Current methods of image protection based on chaos encryption can only provide security in Human visual system (HVS) level, however they cannot provide usage control when the image is opened, printed or exported. Novel image digital rights management scheme for Confidential image data security based on encryption and watermark is used to solve the above problem, wherein full content image encryption for confidentiality to protect the images. Firstly proposed strict and detailed Usage control scheme for Confidential image data (CIData) usage during password-based authentication, opening times, printing and export control. When the CIData need to deliver or export to other users encrypt the image based on AES, after encryption watermark is generated. Both the uploaded image and watermark image is appended together to encode, then the image is splitted into Least Significant Bit (LSB) of randomly selected pixels. Embedding techniques are integrated before the data transmitted to the receiver via the network. The splitted components are transmitted to the receiver. The receiver will download the image which is based on intensity values and combine the image by embedding both user-identification-related and hardware-related records as robust watermark for trace-ability and responsibility confirmation.

IndexTerms **– Encryption, Data Hiding, Digital Rights Management Scheme, Confidential Image Data Security, Watermark.**

I. INTRODUCTION

The main objective of the project is to provide extra security by using AES encryption and watermark for image. By embedding the encrypted image in randomly decided pixels LSB and then splitting the image into parts before the data transmitted through the public network. The security is achieved by splitting the encrypted data and embedded image into parts and then transmit the image parts to the receiver through the public network. To control the secrecy and security of confidential images in various network without being misused or leaked for commercial purpose. By using encryption and watermarking technique can overcome the above issues. Using this process the image can be transferred more securely because before transmitting the images it is splitted into parts based on the intensity values
of RGB components. In this approach decrypt the confidential image data into plain mode and simultaneously embedded both user and hardware related informations as strong watermark for traceability and responsibility confirmation. It evaluates the groups of variant size image data for protection and performance; large amount of agencies prove the above techniques comfortable, secure, efficient, pervasive for confidential image data protection.

1.1 OBJECTIVES

With fast development of computing technology, many images data such as photos, scanned pictures or sensitive diagrams are produced from cameras, scanners, special image or diagram software and devices; are more convenient
to spread and share via online network services. However leakage of commercial, valuable or military sensitive images or diagrams data may lead to serious lost or information security risk. To control and ensure the security of confidential image or diagram data is one of most important issue to be considered. Upon the above problem, much more approaches are studied for image data protection, the most main approach is to encrypt or watermark image data not be visible to Human visual system (HVS); other way may includes isolating the design or process software environment not to link to the internet and then prevent the data from being exploring or shared to public. In fact, even if the image data was encrypted and transfer or export to other users who may use the data without the same encryption computing environment. Then need new approach to protect the image data from being misused, watermarking is a reasonable direction for image data. Traditionally, watermark is employed for authentication or Digital rights management (DRM) of image, when the desired image is to be authenticated; the watermark bits are extracted from the image. Perceptual quality, location capability and security are the most important for the fragile watermark-based image authentication approach. In case of fragile watermark, the robustness is not very important, while robust invisible watermarking is the technique from which it is very difficult to remove the watermark by unauthorized user. Here use hiding of secret message with in an original message and extract it at its destination. It allows embedding different types of information in different types of Medias. It conceals the presence of embedded information with in the media. Another way is the procedure to transform the information to unread format. As a result the interloper cannot read the content of data at first vision. In digital internet domain both techniques are combined to provide more security to the data from the intruder. This combination of techniques provides multiple securities to the data through network. Using these techniques can achieve perfect secure communication. The key will used to encrypt concealed information. Then this cipher data will be embedded to the media which selected to hide the secret data. While transferring the images to the end user first will encrypt the image and then perform watermark technique. Here both the uploaded image and watermark image append together, then the image is splitted based on the intensity values.

2.Literature Survey

Image processing is a way to transform an image into digital form and perform few operations on it, in order to get an enhanced image or to extract some beneficial statistics from it. The purpose of image processing is divided into 5 groups. They are:

1.Visualization - Observe the objects that are not visible
2.Image sharpening and restoration - To create a better image
3.Image retrieval - Seek for the image of interest
4.Measurement of pattern- Measures various objects in an image
5.Image Recognition- Distinguish the objects in an image.

The main image encryption schemes can be classified into different kinds of encryption approaches : partial selective encryption, visual cryptography. Here should discuss the special character of each technology and evaluate
which is suitable for confidential image encryption. The main encryption technologies are discussed and evaluated as following.

Partial selective encryption [1] The cryptosystems based on chaos synchronization were mainly applied in encrypting the sine and cosine signal, simple mixed-signal, text message, and so on. So far, because the image signal has the distinctive function compared with general signal, such as strong correlation among adjacent pixels, great capacity of data, most of next researches classify the partial encryption for digital images into spatial and frequency domains by presenting the parts that are look greater sensitive and needs protections, and then encrypt such parts either by the way of use of decoders or traditional symmetric and asymmetric cipher.

Visual Cryptography [2] The principle of visual cryptography is secret sharing of parts of images to be protected, and when necessary parts of the separated images are combined together to recover the whole original image. One of the best known techniques has been credited to Moni Naor and Adi Shamir developed it in 1994; they examined a visual secret sharing scheme, wherein an image turned into broken up into n shares so that only someone with all n shares could decrypt the image, at the same time any n - 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme such as k-out-of-n visual cryptography. In 2001, Ateniese et al. proposed a scheme that extended capabilities for visual cryptography, Rastislav Lukac and Konstantinos N. Plataniotis proposed a secret sharing scheme capable of
protecting image data coded with B bits per pixel. In 2011, Askari proposed visual cryptography for biometric authentication application, which is good direction in visual cryptography.

Jun Tian et.al in [3] Reversible data embedding using a difference expansion, proposed a reversible data embedding using a difference expansion. The difference of pixels is taken and least significant bits of difference which are all zeros are used for embedding data. It also gives location information that is the information where difference expansion takes place and this will be stored with embedded data. From the location information decoder can restore the embedded data and thus original image can be recovered.

Diljith M. Thodi et.al in [4] Expansion embedding techniques for reversible watermarking, proposed a reversible watermarking method, using a prediction error. Data embedding is done by preserving the information content. It makes decoder easy to extract the watermark and can also perfectly reconstruct the original content. Prediction error is estimated using the pixel intensity and the prediction intensity. The difference of the pixel intensity and the prediction intensity is the prediction error and is used to embed data. Embed data gives watermarked value and embed data is extracted from least significant bit of watermarked value and the original pixel intensity can be restored.

Pramod R Sonawane et.al in [5] Reversible Image Watermarking Using Adaptive Prediction Error Expansion and Pixel Selection, proposed a reversible image watermarking it restore the original image through watermark extracting process. It exploits the spatial redundancy in natural images. Image pixels are categorized into flat and rough region using a threshold. Two methods are used together adaptive embedding and pixel selection. Flat Select region pixels are used to embed two bits and rough region pixels are used to embed one bit. smooth pixels and ignore the rough ones. Rough pixels remain unchanged. Pixels are select according to threshold level. If forward value less than threshold it is smooth pixel otherwise rough. Only smooth pixels are expanded or shifted. Smooth pixels are used to hide more data. Data embedded in smooth areas makes low distortion.

Wei Liu et.al in [6] Efficient compression of encrypted grayscale images, proposed a system for efficient compression of encrypted grayscale images. Resolution progressive compression used to compress encrypted images. Sender transmits down sampled cipher text. Receiver decodes and decrypt with low resolution, from high resolution image get by intra frame prediction. This image combine with encryption key, used as side information to
decode next resolution level and it is repeated until full image is decoded.

Weiming Zhang et.al in [7] Improving various reversible data hiding schemes via optimal codes for binary covers. Proposed a system codes can reach rate distortion bound till compression algorithm reaches entropy. Using binary codes, three RDH schemes can be improved by using the binary feature as covers, an RS scheme for spatial images, one scheme for JPEG images, and a pattern substitution scheme for binary photos. Embedding rates can reach maximum embedding price at the least distortion. This improves the recursive construction and joint encoding.

Zhicheng Ni et.al in [8] Reversible data hiding, proposed a method that describes original image can be recovered without any loss after extraction of hidden data. In this image is encrypted using a key after that embedding data is also encrypted using a data hiding key. The decoder can recover the data only using the data hiding key and after that only original image can decrypt using the key and extract it. Histogram of the image is used to detect the zero and peak points. Data is embedded to only slightly changing values.

3.SYSTEM ANALYSIS AND DESIGN

3.1 EXISTING SYSTEM

In the existing systems, there are many provisions for embedding data. If the image data was encrypted, when the image need to transfer or export to other users who may uses the data without the same encryption computing environment; then it need new approach to protect the image data from being misused. Watermarking is a reasonable direction for image data. Traditionally, watermark is employed for authentication or Digital rights management (DRM) of image or video content. When the desired image is to be authenticated, the watermark bits are extracted from the image to detect the tampered areas. Perceptual quality, location capability and security are the most important for the fragile watermark-based image authentication approach. In case of fragile watermark, the robustness is not very important, while robust invisible watermarking is the technique from which it is very difficult to remove the watermark by unauthorized user. Many fragile or semi-fragile watermarking strategies have been proposed for image content authentication. The delicate watermarking schemes are designed to detect any slight modifications to the bits of the watermarked image and the watermark turns into undetectable after the watermarked image is modified in any manner. The semi-fragile watermarking seeks to verify that the content of the multimedia has no longer been modified by illegitimate distortions, while allowing modification by using valid distortions. In past decades to recent, most researchers on image security mainly focused on chaos encryption such as Logistic and Arnold to protect the image itself. In fact, the principle of chaos encryption is to transfer the pixel to scrambling the data that the image is not visible to HVS, its security is low and not so strong to resist attacks. Current image encryption method never provided usage control mechanism such as control the image data usage times, backup or
export. And moreover, when the image data was misused or leaked and spread to internet, there is no efficient way to find and trace the responsibility and its subjects. To solve the above discussed problem, it is very necessary to study and develop new and efficient solution for confidential image data protection.

The existing systems will embed data in a good and proper way. Data extraction and image recovery are easily done. But the problem is that after embedding data in image, the data is directly transmitted through the public network. This method cannot achieve perfect secrecy. Because if the data is directly send through the network, if there is an attacker in the network gets data hiding key he will tries to extract the data and gets the whole data from the first attempt. So it is not secure to transmit secret data using existing method.

3.2 PROPOSED SYSTEM

Proposed a novel Confidential image data security scheme based on encryption and watermark (CIDSEW) for Confidential image data (CIData) protection, in which for the purpose of image data confidentiality, considering the security of chaos encryption such as Logistic or Arnold is easily to cracked which is not fit for confidential and high level security image data. In this approach full image content encryption and strict usage control for CIData protection opening times, printing and exporting amounts, backup or restore from being illegal leakage or misuse. When the CIData need to delivery or export to other users or other domain, decrypt and export the ciphered CIData to simple mode; and simultaneously we embedded both user-identity-related and hardware related information as robust watermark for traceability and responsibility confirmation. In the proposed method, the data is embedded into an original image. Before data embedding into image, it is encrypted into cipher data using an encryption key. Then encrypted data is embedded into original image pixels. The image is then splitted into parts. The splitted parts are encrypted. Then the splitted parts are send to receiver. Receiver will receive the parts, decrypt it and combine the parts in correct order to form the image without any distraction.
Steps for the proposed method is as follows

Sender side
1. Upload an image
2. Read the data of system and generate watermark
3. Watermark appear in a blank image
4. Embedding watermark image to blank image
5. Encrypt the embedded image using AES encryption
6. Split the image based on the intensity of RGB color component
7. Transmit the splitted image

Receiver side
1. Receives the image data
2. Download the image
3. Combine and rejoin the image based on the intensity values
4. Decrypt the image using AES
5. Decode the embedded data
6. Get the system details

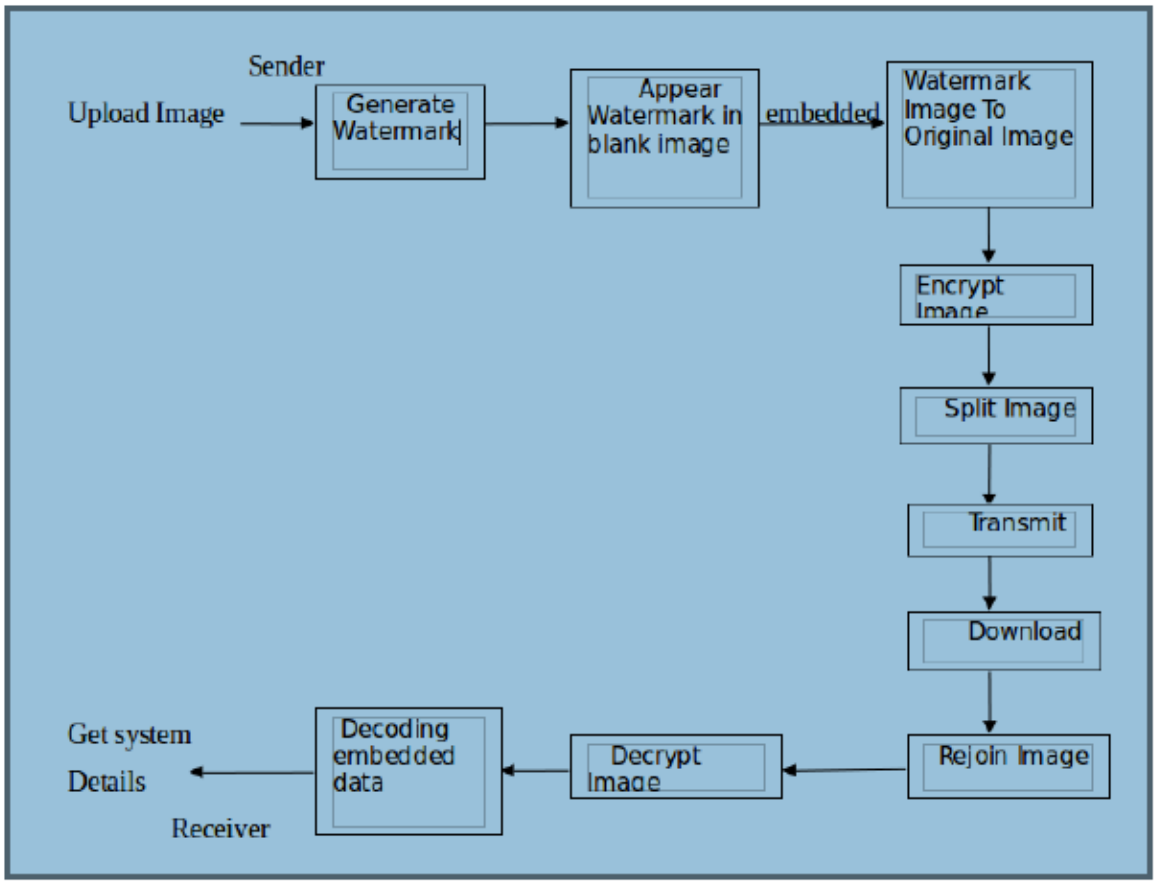

Fig. 3.1: Architecture

Original image is embedded the additional data. By using an encryption key the data is encrypted and embed into image. Reversible data hiding is a technique used to hide the content in original image. By using reversible data hiding technique, the original image is recover and secret data lossless without any error during the extraction. After embedding encrypted data in the original image, then the image is splitted into parts. Encrypt each parts of the image. The encrypted image parts is transmitted through the network. At the receiver side, receives each part. Then rejoin all parts of image at the receiver side.

Proposed method generally consists of four stages

1) Generation and hiding of encrypted data in image

Select an image for data embedding. The encryption method used for data encryption is AES. Secret data, that enter is encrypted using AES. Image, cipher data, and length of cipher data, image lengths are read and stored as byte. If not then only can data embedded to the image. Cipher data length is stored in the first pixels of image. Data embedding is not done in first pixels. If cipher data embed in first pixels continuously it is easy to achieve the data for the intruder. So left some first pixels and then take some pixels randomly from the image using a random function and store it in array. During the random pixel selection, apply some conditions to avoid continuous pixel taking. If condition is not satisfied again call random function to generate another pixel. Thus create pixels for data storage. Method for embedding length and cipher data to pixels is similar. Each byte of data contains eight bits. Then the eight bits of each byte is stored in least significant bits i.e., LSB of eight different pixels. Add or removal of data is taken place at LSB of pixels. Data bit is shifted to its LSB and extract it. During embedding make the pixels LSB into zero value by AND it, then only data can add to that position. To that position data bit can append by OR operation.

2) Splitting of image and its encryption

After data embedding image is split. Each image pixel is the combination of RGB color components. It read and save the intensity values of each pixel. Then separate each color component individually. Take any of the RGB color component intensity range, then pick pixels of image whose intensity values lies in between the range that we take and store that pixels in a blank image. Embed the pixel value to the blank image. So only a small portion of the blank image used to embed the image pixels and remaining portions of the blank image contains pixels without any data. Subsequently encrypt the image part using AES. Similarly using the remaining intensity of pixels creates new image and this process continues till the intensity reaches 200. Thus image is splitted and create the image parts. Each part of the image is the same size of original image. Image fragments number will depends on the intensity range of pixels taken for splitting. Then send the encrypted image parts to receiver.

3) Image decryption

Decryption of image is taking place at receiver side. At receiver side, receiver receives each part of image. Combine the image and then decrypt each part of image. Then RGB components values of each pixel are read and store it in a blank image. Blank image is same as the size of each image part. Similarly from all the image parts take the pixel values and store it in the blank image. Thus combine the image parts to form a single image.

4) Decoding data

First pixels of image contain only message length i.e., first four bytes. Data bits are embedded in the LSB of pixels. So extract data bits from LSB, read and store each LSB bit to an array. If the array reaches eight then we get one byte of data or a character of a data.

4. RESULTS AND DISCUSSION

While uploading an image in the network, watermark is generated of that image by viewing both user-related and hardware-related informations as shown in below figure 4.1.

Fig. 4.1: Watermark Image

Here the image is splitted into parts by taking the intensity value of RGB component. First image part is obtained by taking the intensity from 0 to 50. Result of phase 1 is shown in below fig.4.2 and fig.4.3.

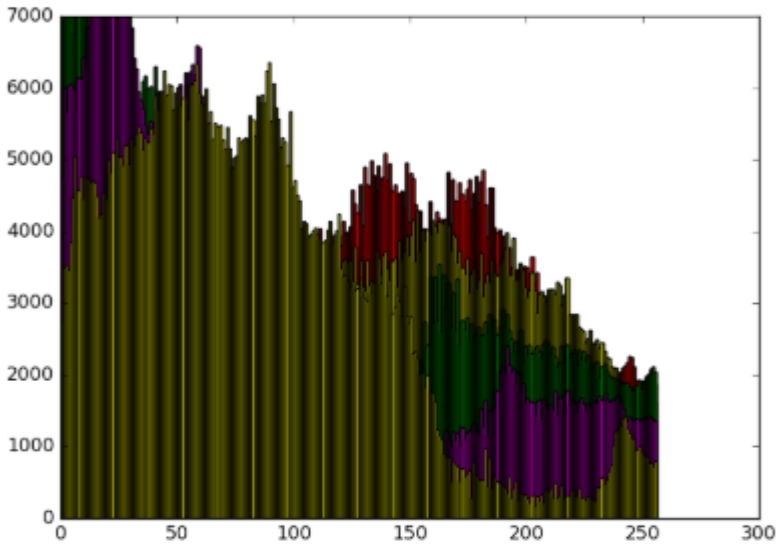

Fig. 4.2: Histogram analysis of Phase 1

Fig.. 4..3: Phase 1 Image

Second part of the image is obtained by taking the intensity value from 50 to 80. Below fig.4.4 and fig.4.5 shows the results of phase 2.

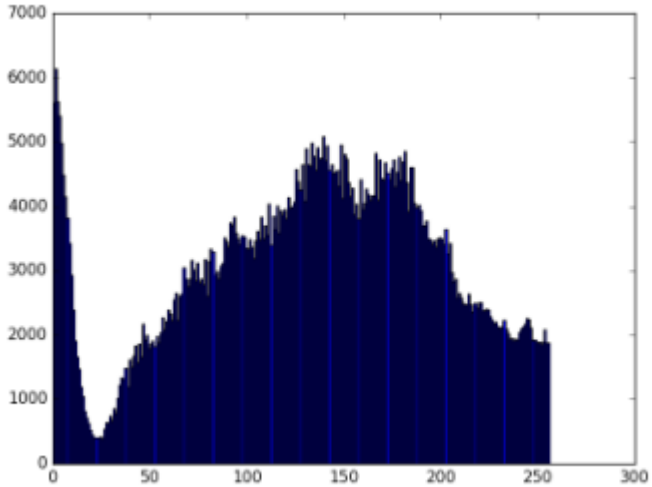

Fig. 4.4 Histogram Analysis of Phase 2

Fig.4.5: Phase 2 Image

Next is the process of generating the third image part, for this take the intensity value from 80 to 120. Below fig.4.6 and fig.4.7 shows the result of Phase 3.

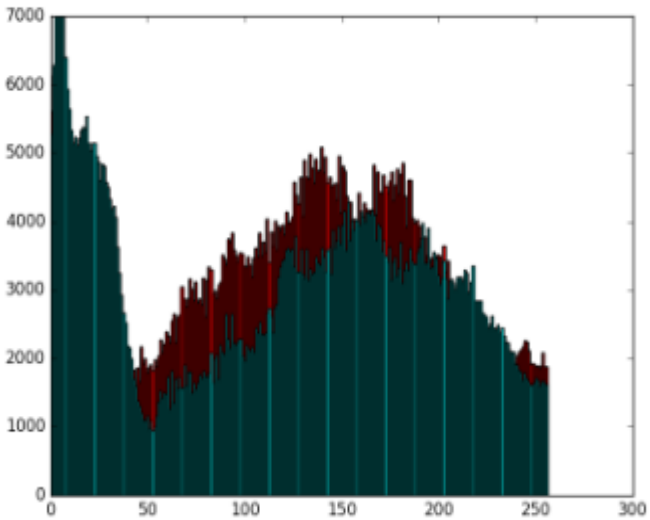

Fig.4.6: Histogram Analysis of Phase 3

Fig.4.7: Phase 3 Image

For generating the fourth image take the intensity value from 120 to 150, Below fig.4.8 and fig.4.9 generates the results of phase 4.

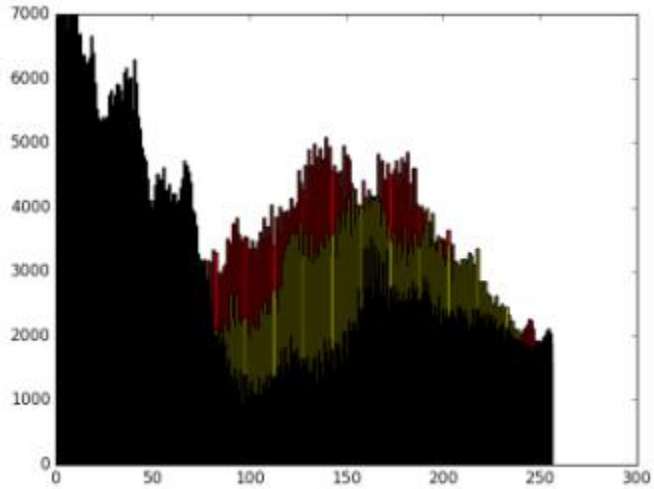

Fig.4.8: Histogram Analysis of Phase 4

Fig..4.9: Phase 4 Image

Phase 5 is the final image state get by splitting the image based on the intensity of 150 to 200. Below fig.4.10 and 4.11 shows the result of phase 5.

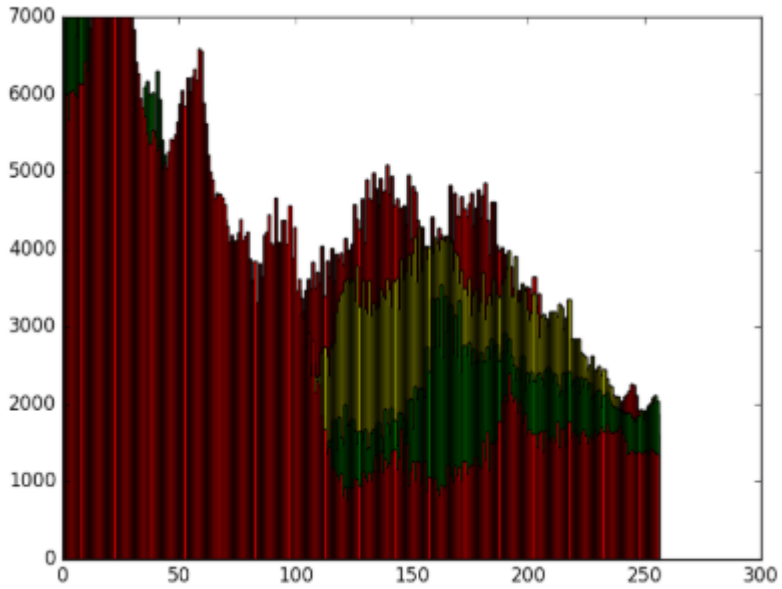

Fig.4.10: Histogram Analysis of Phase 5

Fig.4.11: Phase 5 image

6.CONCLUSION

Novel image digital rights management scheme is proposed for Confidential image data security primarily based on encryption and watermark (CIDSEW) with high-degree security, in which employed full content image encryption for confidentiality of the image. This project specifically focuses on the security of data during the transmission through the general public network. The image is encrypted using AES encryption method, then the cipher data is embedded into randomly generated pixels of an image. After that the stego image is splitted into image fragments and transmitted through the public network. While trying to decrypt the splitted image ,the enduser gets only a part of the embedded data instead of viewing whole data. Robustness of the system is achieved as it is integrated with an advanced encryption standard (AES) and is tested through the histogram analysis. This process can extract original image and secret data accurately and efficiently with high PSNR value of 60dB.

REFERENCES

[1] **Lini Abraham and Neenu Daniel** Secure image encryption algorithms: A review ,International Journal of Science technology, Vol.2, No.4, pp.186- 189, 2013.

[2] **The di_erence between encrypted HLS, PHLS and HLS with DRM** http://www.overdigital.com/online-video/content-protection. 2015-06-18.
[3] **Y. Xu, H.Wang, Y.G. Li, et al.** mage encryption based on synchronization of fractional Commun Nonlinear Science Numeric Simulation, Vol.19, No.10, pp.3735-3744, 2014.
[4] **C.E. Dong,** Color image encryption using one-time keys and coupled chaotic systems,Signal Processing: Image Communication, Vol.29, No.5, pp.628-640, 2014.
[5] **A.K. Osama and A.M. Zin,** An e_cient adaptive of transparent spatial digital image encryption ,Procedia Technology, Vol.11, No.1, pp.288-297,2013.
[6] **Pramod R Sonawane, K.B .Chaudhari,** Reversible image watermarking using adaptive prediction error expansion and pixel selection ,Interna tional Journal Of Engineering Science And Innovative Technology (Ijesit) ,
Volume 2, Issue 2, March 2013.
[7] **W. Hong, T. Chen, and H. Wu,** An improved reversible data hiding in encrypted images using side match,IEEE Signal Process. Letter, vol. 19, no. 4, pp. 199-202, Apr. 2012.
[8] **W. Zhang, B. Chen, and N. Yu,** Improving various reversible data hiding schemes via optimal codes for binary covers, IEEE Trans. Image Process, vol. 21, no. 6, pp. 2991-3003,Jun. 2012.
[9] **X. Zhang,** Separable reversible data hiding in encrypted image, IEEE Trans.Inf.ForensicsSecurity, vol.7, no.2, pp. 826-832, Apr.2012.
[10] **W. Liu, W Zeng, L. Dong, and Q. Yao,** E_cient compression of encrypted grayscale images, IEEETrans.ImageProcess vol.19, no. 4, pp. 1097-1102, Apr. 2010.