Nat. Volatiles & Essent. Oils, 2021; 8(6): 6003-6016

NVEO
Natural Volatiles &
Essential Oils

Security And Preservation For Video Data Transmission Using Blockchain Technology For Cloud Storage On Internet Of Things (Iot)

Dr. K.G.Revathi[1] , Uma Devi.C[2] , S.G.Hymlim Rose[3]

[1]Professor, Electronics and Communications Engineering, DMI College ofEngineering.

[2]PG Scholar, DMI College of Engineering.

[3]Assistant Professor Engineering , St. Joseph College of Engineering.

Abstract:

In Internet of Things (IoT) process, the video transmission handles a security issue in larger extend. Forgery, data theft are some of the issue that should be severely prone the IoT technology. Prior to data storage mechanism, the data is sustained by means of centralized server. In most of the practical situation, encrypted image has to be compressed in order to efficiently secure the data. So that, a pair of image compression and encryption algorithms are designed to perform the operation. In this article, an effective encryption-then-compression (ETC) scheme is designed where they considered both lossy and lossless compression. This approach is driven in the prediction error domain and is reasonably very effective to build high security level. Once the server is influenced by malicious attack, this threatened the security problem in IoT. To outlook the aforesaid security issue, a block-chain based sensingvideo of transmission and storage mechanism is proposed. Initially, the video information is sensed intelligently and splits them into individual blocks. Next, the separated data blocks are encrypted by using intelligent encryption algorithm and then securelytransmitted it. Lastly, the intelligent verification technique is used to confirm the signature verification. This IoT based block- chain is highly reliable, less expensive and effective secure informative data storage when compared to centralized storage mechanism and traditional IoT data transmission.

Keywords — Video Encryption, Block Chain, SPIHT Algorithm, Watermarking, Video Multiplexer, Video De-Multiplexer.

I INTRODUCTION

Everyday ample of data is circulated over the internet. The data so circulated can easily be faked without error, putting the rights of their owners in risk. Even though when encryption is worn in support of distribution, information can

easily be decrypted and then copied. One method toadjourn illegal form is to introduce a watermark duplication, which potentially liable in a way of notdistinct the watermark from the usual data. In original data, the watermark of text or video is embedded into it. This in terms, the authenticity is evidentally maintained over the document. Digital watermarking is the extension of the same notion. There are two forms of watermarks: invisible watermark and visible watermark. In this project wehave focused on unseen watermark. The secret code of either video or text watermark is insert into the video in such a way the corresponding hided code can't be visible by naked eye. It is used to shield the authentication of video and avoid it from being copied. The necessities of watermarking are robustness, perceptual transparency and capacity or pay load. A watermarking system is distributed into two individual steps namely embedding and detection. For embedding process, an algorithm is used which intakes the host video and the data to beembedded and gives a watermarked signal. Thenthe corresponding signal is then transferred to otheruser**.**

Secondly, encryption is the technique which encodes information in such a way that unauthorized parties cannot read it, but onlyauthorized parties can have access to it. Hacking is the unauthorized attacker that can easily corrupt thedata so encryption technique is employed to encrypt the data. In encryption process, the plaintext of information is transferred into ciphertext. This transformation is performed with the help of encryption key, which choose how the data should be encoded. Due to the encoded data, the other unauthorized user can't able to detect the original data within the cipher text. The authorized person from other side can use decryption algorithm of secret key. With this secret key, they can easily find the original message. We have used here blowfish algorithm for encryption which is a symmetric block cipher. This algorithm is more efficient to securely encrypt the data. This algorithm makes use of a varying length of keyranging from 32 bits to 448 bit making it idyllic for the protection of data.

With the rapid evolution of network technology, the internet easily transmit themultimedia information. In military map, the data confidential is most important that transmit over the Internet. The significant consideration arise in this field is security issue, which use secret image for communication. This secret information maynot easily hacked by hackers while they utilized strong communication link over the network. Sothat number of improved image cryptographic algorithms are implemented to securely transmitthe data using secret information.

To secure images, a visual cryptography was developed. Contrast to other cryptographic method, the decryption can be done with manual system without the help of computational system. Nowadays, the data transmission is growing promptly over the network, which offers instantaccess of digital information. The latest technology used a technique called visual cryptography which transmit the secret data in image. In communication technology, production and security, secret image sharing plays an important role in it. However, the security should be deployed in several ways such asimage hiding, password, identification, watermarking and authentication. But the shortcoming arise in this technique is that secret information can't be secured in multi-information carrier. Once the information may lost, the information carrier is either destroyed or damaged. To tackle this difficulty, Naor and Shamir developed a secret sharing VCS technique. In this scheme, the partition process is employed to split the secret image into several shares and transfer them into several participants. By this separation, qualified participants are capable toretrieve the secret image by overlapping the shares in correct order. The conventional VGS applies input as secret data and deliver output as number ofshares. With this hold, the approach fulfils two conditions (i)Any qualified share subset recover thesecret image and (ii) Any forbidden share subset can't improve any details about the secretdata.

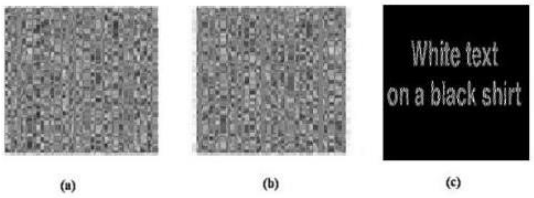


Fig 1. 128x128 image size of conventional (2,2)-VCS

Fig 1. Shows 2 shares of secret image and its splitting process. To distribute the shares, the two participants are used to gain the information without the single participant.

The technique of visual cryptography is to encrypt the data by transparencies from original image. Transparencies is actually a data that should be given to the authorized person and decryption process is performed at the adjacent side of another authorized person. This corresponding process is demonstrated by using tool, which interms the original image is extracted out. In this work, proposes a new visual cryptography and mention how the user examine the encryption and decryption process to secure the image. In this technology, encrypt the image from sender has acquire more than two transparencies of same image. This application emphasis the end user of encryption which drastically split the test imageinto several distinct images. With this application, the secret data of encrypted detail is saved in the extension of PNG and GIF. Finally, the saved encrypted transparencies are sent to the authorized user by source.

Image:

It is a two dimensional signal analyzed by visual manual system. Here, the signal indicates the images that are arranged in analog format. For image processing application, the required analog image is converted into digital image. Additional information is that digital image constitute the two-dimensional pixel array.

In biomedical, remote sensing and video application, digital image plays a significant role in it. The use of and dependence on information and computers continue to grow, so does our need for efficient ways of storing and transmitting large amounts of data.

Image Pixel:

The raster image specifies the digital data whichare arranged in a pixel co-ordinates. Pixel is a smallest unit that corresponds to control the entire image. Pixel address is also called as pixel coordinates that assemble the smaller units as atwo-dimensional grid and is often indicates as squares or dots. A simple compressor and cryptography scheme is depicted in Figure 2.

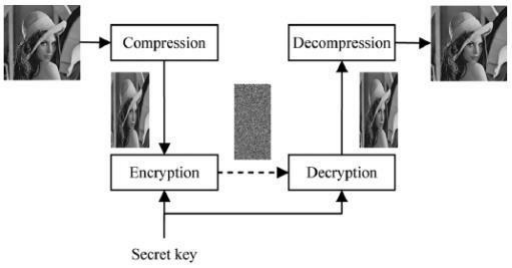


Figure 2. A simple compressor and cryptographyscheme using Lena image

At first, encryption operation takes place. The aim of this process is to change the compressed data to be unreadable and it cannot give required authorization to perceive the other third party. The next step is to minimize the data size as a sufficient level while data transmission take place. This tend to address the process of compression. Due to this compressive process, the unwanted information of

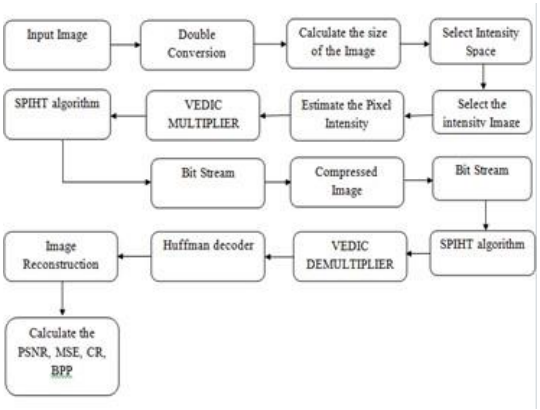
redundancy has to be completely eliminated. Both these operations are performed individually but they intensely bound to control each other. In conventional system, these two operation capable to amalgamate spectral information. This system is based on one hand on the rarity of similitude in two different images and on the second hand on the Discrete Cosine Transformation "DCT", a transformation used for a long time in JPEG compression.

II CHAPTERMETHODS

2.1 BLOCK DIAGRAM & DESCRIPTION

2.1.1. Input Image

To create a 3D imaging, it is applied on the 2D surface by making a depth illusion. It uses a cameralens a make a distance apart to capture the 3Dobject. By the way, the process in intensively replica the human eye vision. The 3D has visually high illusion depth because it represent its two flat surface image as ideally single visible one.



2.1.2 Double Conversion

The given input image is the uint8 data type. The MATLAB will accept the double precision matrix for algorithm development. So we convert uint8 to double.

2.1.3 Compute the image size:

The double precision image is computed by its row,column and dimension arrangement.

2.1.4 Selection of intensity space:

Every image is computed based on its pixel value and is kept within the computer. This value says how the corresponding pixel is looks like. It can be recognized either in the form of color or intensity value. In such case, most of the image are either binary or grey-scale image. The bit number representing the pixel value is termed as binaryimage and single number representing the pixel value is termed as grey-scale image. Mostly, the pixel format is almost byte range and is in the rangeof 8-bit integer. Possibly, mention the value from 0 to 255, here ‘0’ represents the intensity color as black and ‘1’ represents white color.

2.1.6 . Estimate the Pixel Intensity

Compute the total number of pixels present in the image.

2.1.7 Wavelet Coefficients

Wavelet coefficients are used to obtain frequency domain image from spatial domain image and is to estimate the image low and high frequency coefficients.

2.1.8 2D DWT Decomposition

Discrete wavelet transform in 2D is actually2dDWT that usually perform wave transform indiscrete nature by some pre-defined rules. Differ from continuous wavelet transform, DWT decompose the image into orthogonal wavelet set. Also, this discrete time series is implemented continuously and is named asdiscrete-time continuous wavelet transform (DT-CWT).

2.1.9 SPIHT Encoder

SPIHT is expanded as Set partitioning in hierarchical trees mainly used for compression technique. The technique is performed in the form of identifying essential matching across the sub and in an image wavelet decomposition. The specialty of this technique is to encode the three dimensional data in wavelet domain format.

2.1. 10 Bit Stream

Conversion of gray scale image into binary stream.

2.1.11 Image compression

It is a data compression application that encode the test data with some bits. The main of this new image compression technique is to minimize the image redundancy and stored them in an efficient way.

2.1.12 SPIHT Decoder

SPIHT decoding is the process to reconstruct theimage.

2.1.13 Inverse 3D DWT

Convert the frequency domain image into thespatial domain image.

2.1.14 Reconstruction of Image

Reconstruction is actually change the image formatfrom double precision to uint8 type.

2.1.15 MSE and PSNR

It is a measuring parameter employed to check thequality of resultant compressed image.

III CHAPTER

3.1 EXISTING SYSTEM

In previous work, the security is only implemented. The existing system focuses mainly on the different kinds of video encryption and decryption techniques. In addition focuses on videoencryption techniques. Day by day advancement in transmission and storage of digital technology, the integrity,

confidentiality and authenticity of video bear an unreliable issue in the current scenario.

3.2 Disadvantages of Existing System

In the existing system, the encrypted video is easilypossible to hack by the intruders. The existing system consists of lossless video compression. Thecompression ratio of the existing system is very poor. The quality of the video after compression is measured and it is very poor in terms of PSNR.

3.3 PROPOSED SYSTEMProposed Algorithm 1

2D – 3 Level Wavelet Transform is used for Video Watermarking

Proposed Algorithm 2

Video Encryption using Lagrange Theorem

Proposed Algorithm 3

Video Compression using Modified SPIHT (Set Partition In Hierarchy Tree) algorithm with Huffman coding

3.3.1 PROPOSED ALGORITHM 1

Video Watermarking is designed by the technique of 2D – 3 Level Wavelet Transform

This proposed system uses a 3 Level Wavelet Transform to design the video watermarking and the evaluated result of 3level DWT is compared against the 1 and 2 levels of DWT. This approach use alpha bending technique that has a characteristics to embed the multiple bit of watermark into the low frequency (LF) sub-band ofvideo. At the time of embedding process, the original image is dispersed by watermark video dueto scaling factor. Finally, as per the same scaling factor, the watermark video has to be extracted.

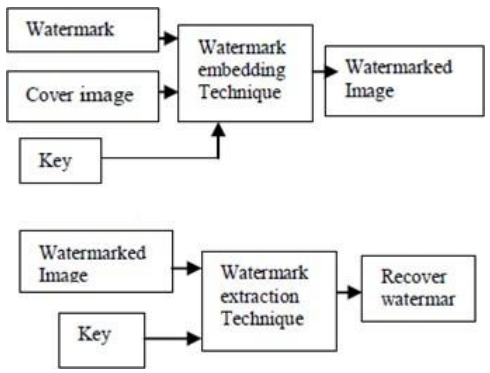


Figure: 2 D – 3 Level Wavelet Transform is usedfor Video Watermarking

The performance is measured for varying scaling factor and is evaluated and compared against the first level and second level of DWT approach by using statistical parametric measure of mean squareerror (MSE) and peak signal to noise ratio (PSNR)

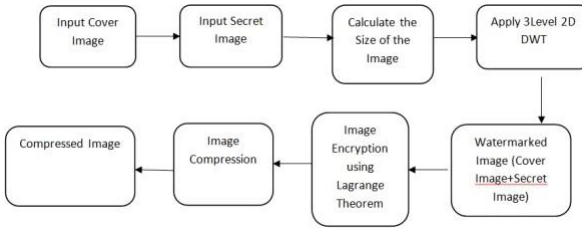


Fig: Block Diagram of Video Watermarking

3.3.1 .1 Input Image

To create a 3D imaging, it is applied on the 2D surface by making a depth illusion. It uses a cameralens a make a distance apart to capture the 3D object. By the way, the process in intensively replica the human eye vision. The 3D has visually high illusion depth because it represent its two flat surface image as ideally single visible one.

3.3.1.2 Double Conversion

The given input image is the uint8 data type. The MATLAB will accept the double precision matrix for algorithm development. So we convert uint8 to double. Calculate the size of the Image Calculate the number of row and column and dimension of the give double precision image.

3.3.1.3. Selection of intensity space:

Every image is computed based on its pixel value and is kept within the computer. This value says how the corresponding pixel is looks like. It can be recognized either in the form of color or intensity value. In such case, most of the image are either binary or grey-scale image. The bit number representing the pixel value is termed as binaryimage and single number representing the pixel value is termed as grey-scale image. Mostly, the pixel format is almost byte range and is in the rangeof 8-bit integer. Possibly, mention the value from 0 to 255, here '0' represents the intensity color as black and '1' represents white color.

3.3.1.4 Select the intensity Image:

For RGB color space, color image is detailed for each pixel and is separated by red, blue and green components of intensity range. With this formation,three co-ordinates is combined to arrange the pixel value as vector.

3.3.1.5 Pixel intensity computation:

At first, the entire pixels are computed in the image.

3.3.1.6 Wavelet Coefficients:

Wavelet coefficients are used to obtain frequency domain image from spatial domain image and is to estimate the image low and high frequency coefficients.

3.3.1.7 2D DWT Decomposition

Discrete wavelet transform in 2D is actually2dDWT that usually perform wave transform indiscrete nature by some pre-defined rules. Differ from continuous wavelet transform, DWT decompose the image into orthogonal wavelet set. Also, this discrete time series is implemented continuously and is

named as discrete-time continuous wavelet transform (DT-CWT).

3.3.1.8 SPIHT Encoder

SPIHT is expanded as Set partitioning in hierarchical trees mainly used for compression technique. The technique is performed in the form of identifying essential matching across the sub and in an image wavelet decomposition. The specialty of this technique is to encode the three dimensional data in wavelet domain format.

3.3.1.9 Bit Stream

Conversion of gray scale image into binary stream.

Image compression

It is a data compression application that encode the test data with some bits. The main of this new image compression technique is to minimize theimage redundancy and stored them in an efficient way.

3.3.1.10 SPIHT Decoder

SPIHT decoding is the process to reconstruct the image.

Inverse 3D DWT

Convert the frequency domain image into thespatial domain image.

Reconstruction of Image

Reconstruction is actually change the image formatfrom double precision to uint8 type.

3.3.1.11 MSE and PSNR

It is a measuring parameter employed to check thequality of resultant compressed image.

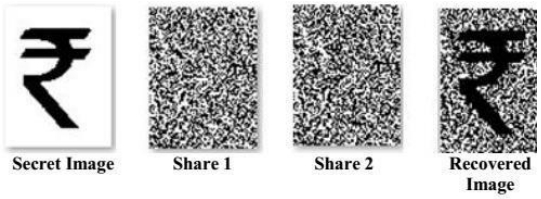
3.3.2 PROPOSED ALGORITHM 3

3.3.2.1 Lagrange encryption technique:

Here, a new approach of video encryption technique is proposed using Lagrange theorem. It comprise of two replacement techniques that has a specialty to modify the pixel value without shuffling it. To fix this, a pixel mapping table is introduced to improve the video uncertainty by random shifting. After then, the replacement technique is imposed to change the row and columnpixels.

Visual cryptography is an encryption and decryption approach used to hide the data and afterwards, the data is decrypted using secret key. In this scheme, several shares are taken from secret data, each of which can't offer any informationabout the secret data. Based on this, only the secret information has to be retrieved where they are superimposed each shares with one another. At the time of decryption, transparency paper is prepared by shares and require to arrange the needed transparencies with one by one that depicts the information. However, the technique need not have any difficult computation like several conventional cryptography approaches. Naor and Shamir designed a new concept in VC scheme where they offer shares for binary data. So that two shares of share 1 and share 2 is generated. The condition is that, if the pixel intensity is black, then bottom row is chosen as any one row where it offer share 1 and share 2. Likewise, if the pixel intensity is white

then top row is chosen as any one row where it offer share 1 and share 2.



3.3.3 PROPOSED ALGOEITHM 3

Nowadays, the computer usage goes on increasing in appropriate level and used in huge number of tasks. Most common usage in digital camera is that they have manipulating, storing and transferring capabilities. The folder that hold all videos but it could be quite large since it suddenly occupies the precious memory space and suffer from data storing lackage. In multimedia field, mostly the videos comprise of huge redundancy so that they also occupies huge space. Therefore, SPIHT is introduced in the video compression concept to done quick and reduced storage space capability. Additionally, the technique exhibit better video quality, quick execution time and enhanced compressed ratio.

In simulation section, the experiment is examined carefully and numerical outputs are processed using matlab software. Finally, the corresponding performance is analyzed using Compression Ratio (CR) and Peak Signal to Noise Ratio (PSNR).

IV CHAPTER

4.1 RESULTS AND DISCUSSION

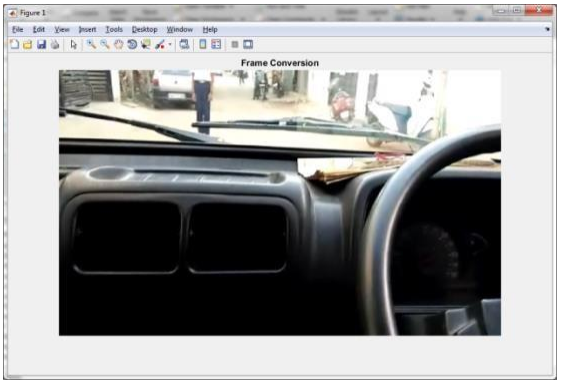


Figure 1: Input video and video to frame conversion

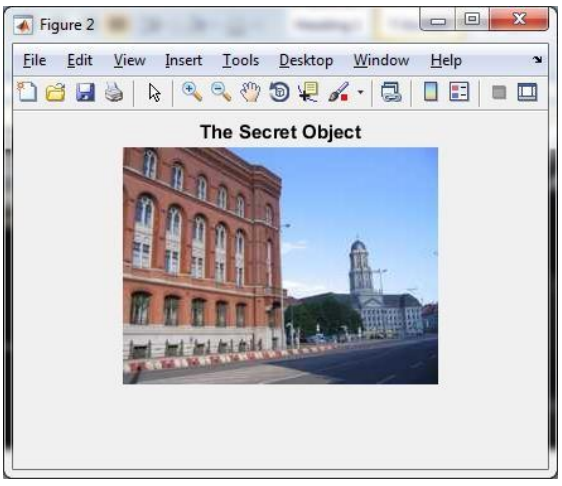


Figure 2: Secret Image to be embedded on the inputvideo

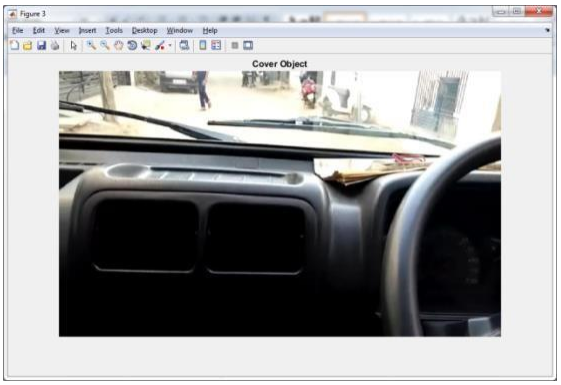


Figure 3: Cover object in which the secret objecthas to be embedded

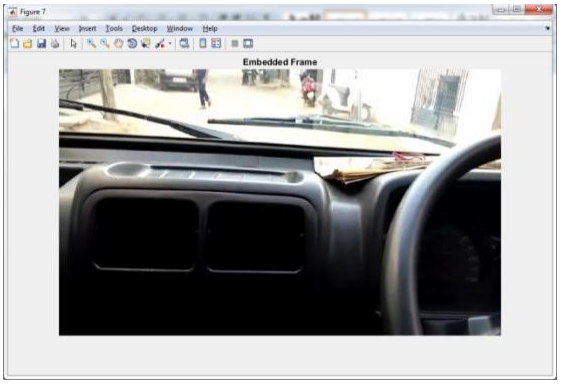
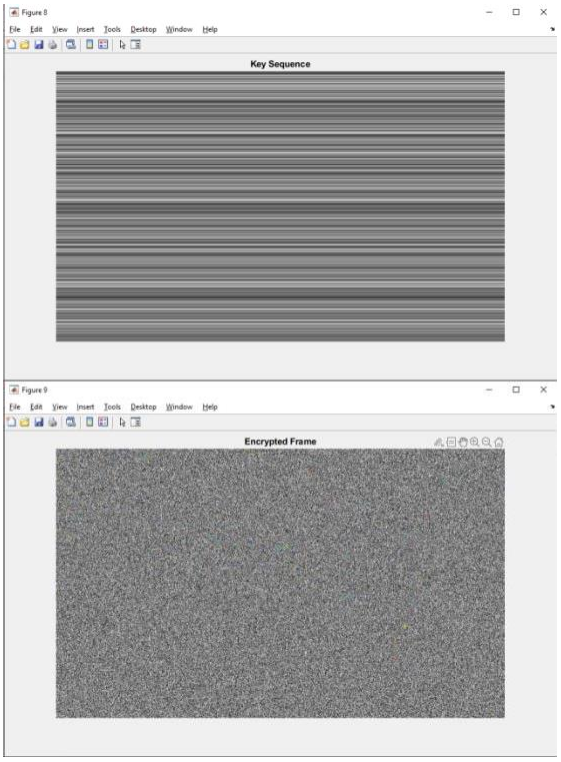
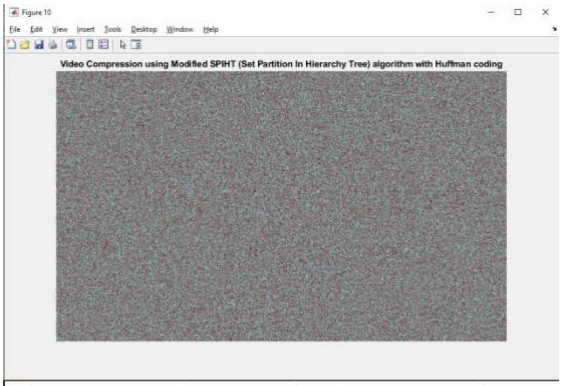
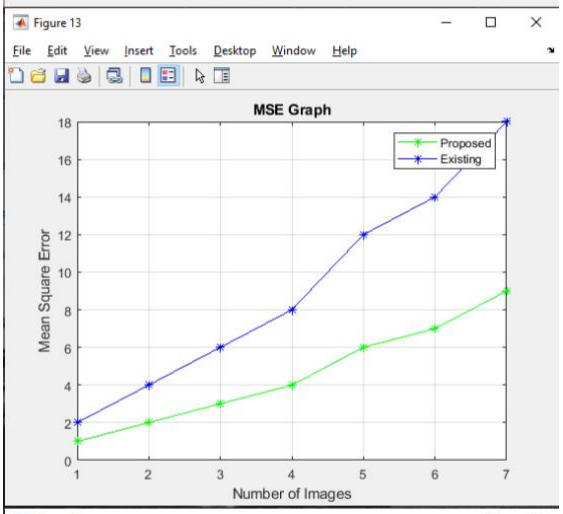
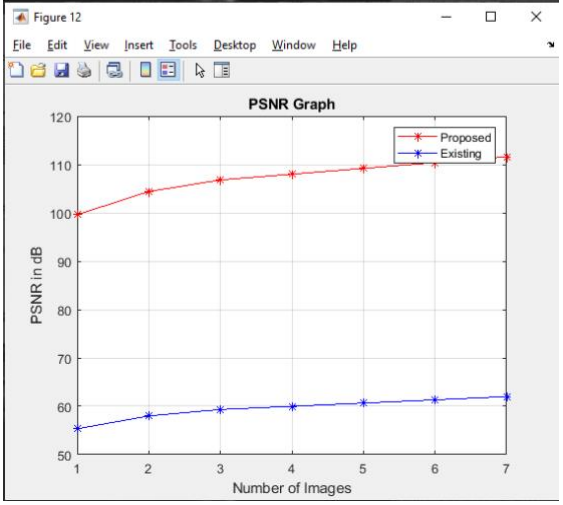


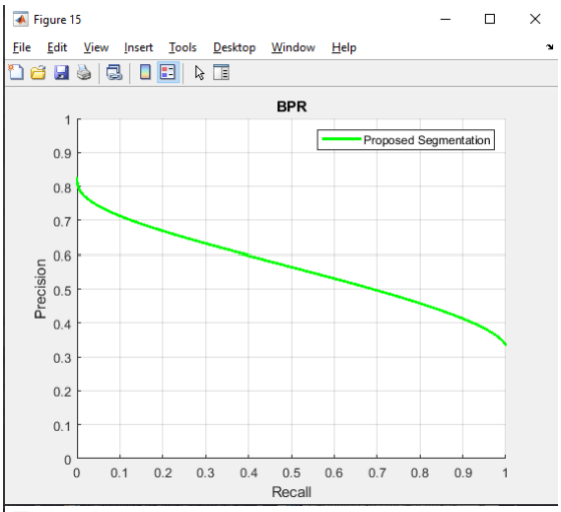
Figure 5: Watermarked Structure

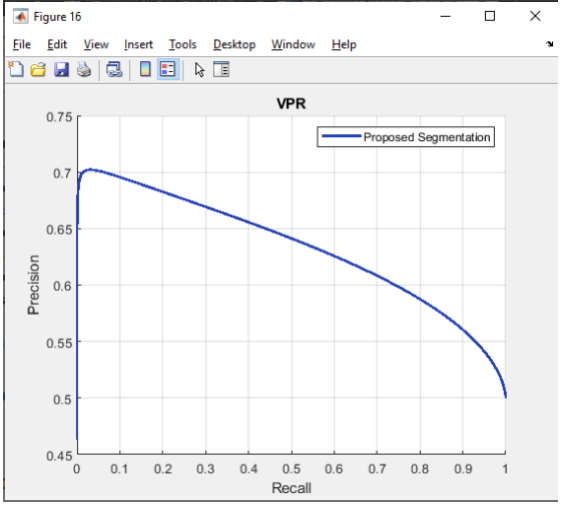












$$BER = \frac{B_{error}}{B_{total}} \times 100\%$$

(38)

where B_{error}

and

B_{total}

denote the number of error
bits and the number of total bits, respectively. Based on the same technique of quantization, we contrast our technique against the one proposed by Lin et al. [18]. Besides, we also contrast our technique against the traditional method which used single-coefficient quantization index modulation, i.e.,

k 1, S 15 .

The test of robustness supports the following conclusions.

In this section establish few investigations to compute the proposed method performance. For instance, the weighting matrix is represented by,

W_1 [1 1 1 1]

matrices

.

CONCLUSION

Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the image areas where a disturbance can bemore easily hidden. Decryption part of visual cryptography is based on OR operation, so if aperson gets sufficient k number of shares; the image can be easily decrypted. In this current work,with well-known k-n secret sharing visual cryptography scheme an enveloping technique isproposed where the secret shares are enveloped within apparently innocent covers of digital pictures using LSB replacement digital watermarking.

This adds security to visual cryptography technique from illicit attack as it befools the hackers' eye. The image is splited into several shares by random number generator, which is anew technique not available till date. SPIHTalgorithm can be used for any video size. When the size of the colour video increases, the time requiredfor compression and reconstruction of the image

and W_2 0.7 1.2 1.3 0.8

also increases. The results show that we obtained improvement using Modified SPIHT
Huffman

However, the results of column three in Table I show that the watermarked image with
$k = 4,\ S = 60,\ W_2$
has lower PSNR than the one with
$k = 4,\ S = 60,\ W_1$.

In figure 3, it represents the Lena image and Jet image. Watermarked image with varying weight matrices are revealed in Figure 4-7. In this case,
$k = 4,\ S = 60,\ W_1$,
the relation between the weight of some coefficient and PSNR are shown in Figure 8 and Figure 9. One can see that the PSNR declines when the weight of some coefficient increases.
In embedding process, the secureness is to be checked so that bit error ratio (BER) is employed to detect the robustness of the system. BER isexpressed as, algorithm in terms of compression ratio, mean- squared error, and Peak signal to noise ratio, correlation coefficient and multi-scale structural similarity index. We can propose a lossless compression method for video.

FUTURE WORK

The reconstruction of the original secret object has to retrieve using reverse process of image watermarking, image decryption and image decompression.

REFERENCES

[1] J. Zhou, X. Liu, and O. C. Au, “On the design of an efficient encryption then-compression system,” in Proc. ICASSP,2013, pp. 2872–2876.

[2] T. Bianchi, A. Piva, and M. Barni, “On theimplementation of the discrete Fourier transform in the encrypted domain,” IEEETrans. Inf. Forensics Security, vol. 4, no. 1,pp. 86–97, Mar. 2009.

[3] T. Bianchi, A. Piva, and M. Barni, “Encrypted domain DCT based on homomorphic cryptosystems,”EURASIP J. Inf. Security, 2009,Article ID716357.

[4] T. Bianchi, A. Piva, and M. Barni, “Composite signal representation forfast and storage-efficient processing of encrypted signals,” IEEE Trans.Inf. Forensics Security, vol. 5, no. 1, pp. 180– 187, Mar. 2010.

[5] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, “Privacy- preserving ECG classification withbranching programs andneural networks,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 2,pp. 452–468, Jun. 2011.

[6] Shruti Goel , V. K. Panchal,” Performance Evaluation of a New Modified Firefly Algorithm” IEEE 978-1-4799-6896-1/14,2014.

[7] Jiantao Zhou, Xianming Liu,” SecureReversible Image Data Hiding overEncrypted Domain via Key Modulation”, IEEE Transactions on Circuits And Systems for Video Technology, 2015.

[8] Swetha Dodla and Y David Solmon Raju,” Image Compression using Wavelet andSPIHT Encoding Scheme”, International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 9-Sep 2013.

[9] S.Sulochana and R.Vidhya,” Texture Based Image Retrieval Using Framelet Transform–Gray Level Co-occurrence Matrix(GLCM)”, International Journal of Advanced Research in Artificial Intelligence, Vol. 2, No. 2, 2013.

[10] Ming Zhang and Bahadir K. Gunturk,” Multiresolution Bilateral Filtering for Image Denoising”, IEEE Transactions onImage Processing, Vol. 17, No. 12, December 2008.

[11] Shivani Sharma and Gursharanjeet Singh Kalra,"An Image Denoising Framework with Multi-resolution Bilateral Filtering and Normal Shrink Approach" Research Journal of Applied Sciences, Engineering and Technology 7(6): 1054-1060, 2014 ISSN: 2040-7459, e-ISSN: 2040-7467.

[12] Sushil Kumar,"A Comparative Study of Transform Based on Secure Image Steganography", ijcce.2015.v4.389,December 16, 2014.