IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 3 (Mar. 2013), ||V1|| PP 10-17

Haze Removal of Secure Remote Surveillance System

Anitharani.M and Padma.S.I
M.Anitharani M.E student is with the department of Electronics and Communication, PET Engineering College, Vallioor.
S.I.Padma assistant professor is with the department of Electronics and Communication, PET Engineering College, Vallioor.

***Abstract*:** A reliable method for dehazing image and video was proposed. The goal is to achieve good dehazed images and videos with proper security at the receiver side. The image was dehazed by dark channel prior. The system based on fast single image dehazing and here the codecs used is joint photographic expert group. Then the compressed image is extended to compressed video, by using codecs H.264. Then by considering the dehazing effects before or after compression, the coding artifacts and motion estimation were investigated. Before compression produce better dehazing performance with fewer artifacts and better coding efficiency than after compression. By using these methods, the thickness of haze and haze free images and videos can be estimated directly. Then a watermark is added for digital right management and the watermarked image and videos is encrypted with a fast and reliable light weight algorithm. This image and video is transmitted to the receiver side. At the receiver side, the use with correct key can decrypt the image and the image will be watermarked with watermark symbol, the watermarked image can be used to trace illegal distribution. Thus this system produces a dehazed image and video with high secure and fast transmission.

Index Terms: *Dehazing, Watermarking, Rate-distortion, and Key-management.*

I. INTRODUCTION

Haze is traditionally an atmospheric phenomenon where dust, smoke and other dry particles obscure the clarity of the sky. This paper presents a combination of special methods for pre and post processing of still images and videos, aimed at compression ratio enhancement and quality improvement of images and video. The pre-processing is based on the image and video restored before compression and the post processing restored after compression. Secure transmission of digital video has long been a top priority for Military application, and is an increasingly important issue for commercial TV

Broadcast and network- based multimedia applications. Such as HDTV (High Definition Television), VOD (Video on Demand), PPV (Pay per View), DVD (Digital Video Disk), online video games and so on.In section II, will give an overview of haze removal of secure remote surveillance system, which is used to protect the dehazed image and videos. In section III, to investigate what happens the images and videos, when it is applied pre and post compression. In section IV, secure remote surveillance system produces based on key-code watermarking, which is used to trace illegal distribution. Then follow with section V, discussed the result for subjective and objective analysis. Then conclude this paper in section VI.

II. OVERVIEW OF THE SYSTEM

The inter-frame motion for dehazed images developed the technique based on dividing a frame into smaller rectangular blocks and finding the direction of minimum distortion (DMD) for each block [1]. To reduce the blocking artifacts, the human visual system (HVS) method will be used [2].The most commonly used methods for image compression are closed-form expressions for compressed medical images. It require large amount of memory space [3].Gary level grouping (GLG) is a general and powerful technique and it used to apply to a broad variety of low contrast images [4].The extension of basic GLG algorithm used to break the gray scale into two or more segments and each segment perform the basic concept when to treat the X-ray images [5].

To enhance the contrast DCT domain, the simple, adaptive and easy to implement with great potential for enhancing the quality of medical images are used [6]. The selective encryption algorithm is used to secure the MPEG transmissions [7].The problems of the MPEG video encryption algorithm are discussed by using random permutation list instead of zigzag order within the MPEG compression [8].The two way selective encryption algorithm for the video is developed to compromise the security and speed in the process of encryption [9].To keep continuous security, key management is also an essential part of the system, that needs three kinds of keys [10]. A dark channel prior is used to remove the haze from single input image [11].The overview of H.264/AVC is used to achieve a significant improvement in rate distortion theory [12].The new motion compensation technique is used to overcome the large calculation of time complicated motion vector

prediction algorithm[13].The adaptive fuzzy filter improves both visual quality and PSNR of compressed images and videos[14].The formation of a haze is contributed by direct attenuation and absorbed other directions[15].The scrambling key is used to conjunction and protecting the digital video streams from un authorized viewing [16].

III. HAZE REMOVAL ON IMAGE AND VIDEO CODING

In fig 1 represented the block diagram for haze removal of image and video coding. Here the input of image/video is in the form of haze. Then the dehazing applied two different methods. First approach is pre compression; it means the dehazing technique applied after compression. Dehazing techniques are dark channel prior and median dark channel prior. Then the result applied to compression standards for image in JPEG and video for H.264. The post compression is first input image/video applied to dehazing techniques before compression. The ringing and blocking artifacts can be reduced by choosing a lower level of compression. They may be eliminated by saving an image using a lossless file format. So, the pre compression is gives better performance and fewer artifacts than the post compression.

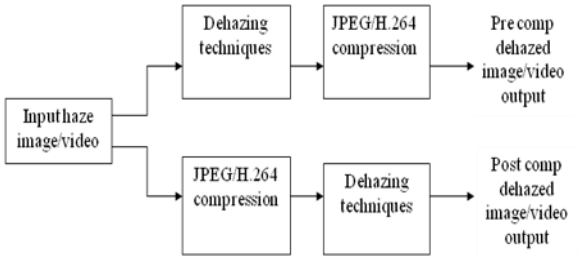


Fig 1.Haze removal on Image and video coding

A. Dehazing Techniques

In image, the fast single image dehazing techniques are used. Here the dark channel prior is simple but effective image prior. The concept of dark channel is an arbitrary image J and its dark channel is J^{dark} is given by,

$$J^{dark} \underset{y \in \Omega(x)}{min} \left(\underset{c \in \{r,g,b\}}{min} \right) J^c(Y) \quad (1)$$

Where, J^c is the colour channel of J and $\Omega(x)$ is a local patch centred at x. the intensity of J's dark channel is low and tends to be zero: $J^{dark} \rightarrow 0$. This is called by dark channel prior. The DCP is constructed as

$$\theta_D(m,n) = \underset{k,l \in \Omega(m,n)}{min} \left(\underset{c \in \{r,g,b\}}{min} \frac{\hat{x}(k,l,c)}{a(c)} \right) \quad (2)$$

But the DCP has the limitation of halo effects for not refining. So, the initial atmosphere scattering light through median filtering is included, to refine the transmission. Compared with DCP dehazing methods, the MDCP method could get a better dehazing effect at distance scene and places. The proposed MDCP is constructed as,

$$\theta_M(m,n) = \underset{k,l \in \Omega(m,n)}{med} \left(\underset{c \in \{r,g,b\}}{min} \frac{\hat{x}(k,l,c)}{a(c)} \right) \quad (3)$$

Where,

θ_D =mostly dark image/video, $\hat{x}$=hazy image/video, Ω = square shape, a = atmospheric light, (m, n) = pixel location, θ_M = mostly bright image/video.

In video dehazing, the compressed image was extended to compressed video. The video sequences are plays an important role in commonly used codecs e.g., MPEG-4 and H.264. A block matching algorithm is the popular choice of reducing temporal redundancy between frames in video compression. Then by apply the MDCP method on a video sequence before and after compression. Here using codecs are H.264 with varying bitrates.

B. Compression Standards

In this haze removal of image and videos technique, joint photographic expert group (JPEG) and H.264 compression standards are used. Compression technique is used to reduce the block size of image and videos. The JPEG compression is used in a number of image file formats. It is most common format for storing and transmitting photographic images on the World Wide Web.H.264 is currently one of the most commonly used formats for the recording, compression and distribution of high definition video. It is a block- oriented motion-compensated-based codec standard it is also widely used by streaming internet sources such as videos.

C.PSNR Performance

Two common measures of image quality are the mean square error and peak signal-to-noise ratio. The PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. It is most commonly used as a measure of quality of reconstruction of lossy compression code. The signal in this case the original data and the noise is the error introduced by compression.

The PSNR is most easily defined via the mean squared error (MSE), which for two mxn monochrome images I and K where one of the image is considered a noisy approximation of the other is defined as,

$$MSE = \frac{1}{mn}\sum\sum[I(i,j) - K(i,j)]^2 \qquad (4)$$

The PSNR is defined as,

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \qquad (5)$$

$$= 20.\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \qquad (6)$$

$$= 20.\log_{10}(MAX_I) - 10.\log_{10} MSE \qquad (7)$$

Here, MAX_I is the maximum possible pixel value of the image. The PSNR is usually expressed in terms of the logarithmic decibel scale.

IV. SECURE REMOTE SURVEILLANCE SYSTEM

Encryption is used to select a Frame. It performs bitwise XOR for Key frame and selected frame to get encrypted frame. Then for more security transposition is also used. The watermark embedding is selecting a watermark image and converted into binary image (0's & 1's) for hiding and adds it to original Frame. The perform Bitwise XOR for watermarked frame and encrypted frame gives the modified key. Inverse transposition is done and encrypted Frame is obtained by using decryption process. It perform bitwise XOR for Key frame and considered encrypted frame to get decrypted Frame consider an encrypted Frame and perform bitwise XOR with Modified Key to get decrypted watermark frame. Then subtract the decrypted frame and decrypted watermark frame gives watermark image. It gives the final protected dehazed image and videos. This is shown in fig 2.

The process involved three main modules, they are

1. Transmission
2. Reception
3. Authentication

A. Transmission

In transmission side the video is encrypted and watermarked. The key to b distributed is also generated. In transmitter there are eight process involved. The eight processes are explained below in detail manner.

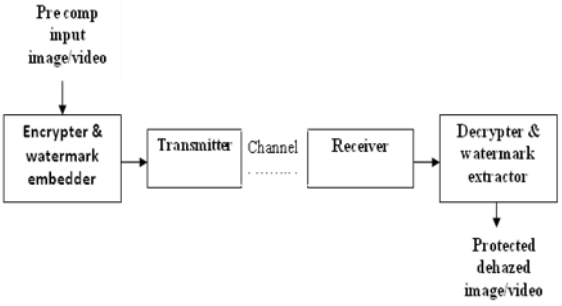


Fig 2 Secure Remote Surveillance System

(1) Video Frame Conversion

In general, video is a collection of frames. A single frame is nothing but an RGB image. And thus a consecutive frames are makes a single video.

If we want to do any video related process, we have to separate each and every frame. Each frame is stored separately. Then each frame is again separated to red, green and blue. Because, any operation or process to be done in entire video. It is absolutely equal to that of the same on all the frames individually.

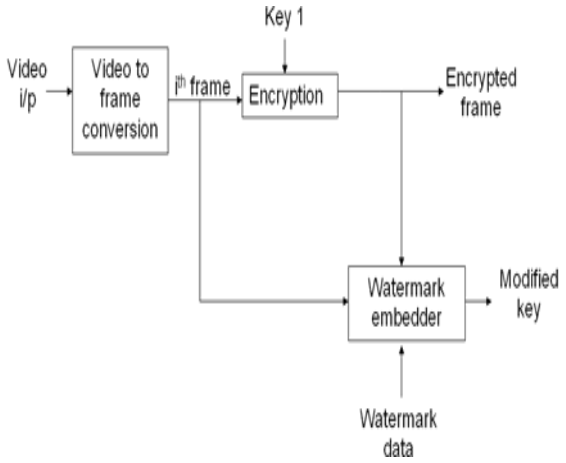


Fig 3 Block diagram for transmitter

(2) Key Frame Generation

Key is simply the data in the form of matrix which is involved in the encryption of the original data. Here, the original data is the frame extracted from the video. The security of the content will be purely based on the key. If the difficult in the generation of the key is more than to hack the data from the system also increase.

Here, we have to extract the key for encryption. With a single 2x2 matrix data, we should generate a key frame of the size of the original frame to be encrypted using various matrix operation. Thus, the key frame has the size equal to the size of the original frame.

(3) Encryption

Encryption is the process in which the original data will be converted into another format with the help of the key generated. It is mainly used for the security purpose. The hackers cannot get any information from the encrypted data. Thus, it provides security to our binary data. Here, we have to provide that security for our video. For this purpose, we use the XOR encryption for fast processing. In general both the frame and the key are numerical data in the matrix format. So, each and every pixel in the original frame is XORed correspondingly with the pixels in the key frame.

$R'_{ij} = (R_{ij})\ XOR\ (K_{ijr})$

$G'_{ij} = (G_{ij})\ XOR\ (K_{ijg})$

$B'_{ij} = (B_{ij})\ XOR\ (K_{ijb})$

Where,

R_{ij}, G_{ij}, B_{ij} →Original Frame.

$K_{ijr}, K_{ijg}, K_{ijb}$ →Keys for Encryption

$R'_{ij}, G'_{ij}, B'_{ij}$ →Encrypted Frame.

The resultant image will be the encrypted image of the original frame. No one can extract the original frame from that encrypted data without knowing the exact key frame.

(4) Generation of Watermarking Data

In this project, we have used the RGB image as the watermarking data. Using this image directly for watermarking it may change the content of the original frame. To avoid this problem, here we have first converted the RGB image into gray image and then this gray image to binary image, and, this binary image is used as the watermarking data. The reason behind this is, the binary image will have the value of '0's and 1's. So there will not be much change in the original frame due the single level change and the watermarked frame look very similar to that of the original frame.

(5) Watermark Embedding

Once the watermark data is ready we can directly use bitwise addition to add the original frame and watermark data. The watermarking here we have used in the invisible watermarking. The segmented R, G, B frame will be added with the extracted binary image of the watermarking data. The resultant R, G, B component of the frame will contain the watermarking data which is invisible to the users, because of the single bit change in the LSB alone.

$W_fR_{ij}= (R_{ij} + Nr)$
$W_fG_{ij}= (G_{ij +} Ng)$
$W_fB_{ij} = (B_{ij +} Nb)$
Where,
R_{ij}, G_{ij}, B_{ij} →Original Frame
N_r, N_g, N_b →Watermark Strength
W_fR_{ij}, W_fG_{ij}, W_fB_{ij} →watermarked frame.

(6) Modified Key Generation

In order to extract the watermarked frame in the receiver, they have to extract the original video from our encrypted frame. For this purpose we have to generate a key to do this process. That key is called as modified key. The modified key is obtained by performing the bitwise XOR operation between the watermarked frame and our original frame with watermarking data.
$M_{ijr} = W_fR_{ij}$ XOR R'_{ij}
$M_{ijg} = W_fG_{ij}$ XOR G'_{ij}
$M_{ijb} = W_fB_{ij}$ XOR B'_{ij}
Where,
M_{ijr}, M_{ijg}, M_{ijb} →Modified Keys
R'_{ij}, G'_{ij}, B'_{ij} →Encrypted Frame
R_{ij}, W_fG_{ij}, W_fB_{ij} →watermarked frame.

(7) Transposition

In order to increase the security of the encryption we have also included transposition in the transmitter side the encrypted frame is scrambled and it is made more degraded such that the hacker may not get any idea regarding the data transmitted

(8) Frame to Video Conversion

The frames that have been processed must be grouped and made into a video before transmission. So, the processed transposition frames have combined to form the encrypted video. These encrypted video is transmitted to the user.

B. Reception

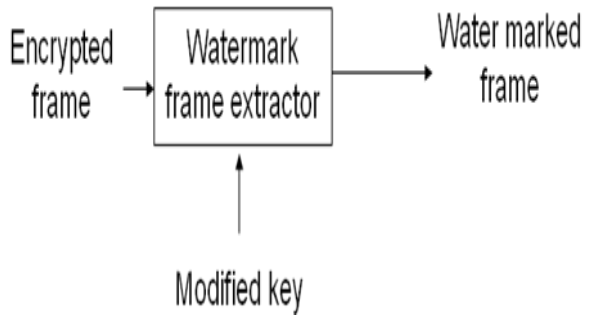


Fig 4 Block Diagram for Reception

In the receiver side the receiver only contains the encrypted watermarked video, along with the modified key. The operation carried in the receiver side in exactly reverse of the transmitter side. We have to segment the encrypted video into numerous separate frames and that frames are converted into R, G, and B components. Then the resultant frame should be reassembled before decryption. Then with the help of the modified key and the encrypted frame we can obtained the watermarked frame using,
$W_fR_{ij}=M_{ijr}$ XOR $R'ij$
$W_fG_{ij}=M_{ijg}$ XOR G'_{ij}
$W_fB_{ij}=M_{ijb}$ XOR B'_{ij}
Where,
M_{ijr}, M_{ijg}, M_{ijb} →Modified Keys
R'_{ij}, G'_{ij}, B'_{ij} →Encrypted Frame
W_fR_{ij}, W_fG_{ij}, W_fB_{ij} →watermarked frame.
Finally, resultant frames are combined together and formed the original video with invisible watermarking.

C. Authentication

This was the section related to the copyright protection. In case of any doubt regarding the illegal distribution of that particular video, the watermark should be extracted at the receiver side. This can be done by using both the modified key and the original key.

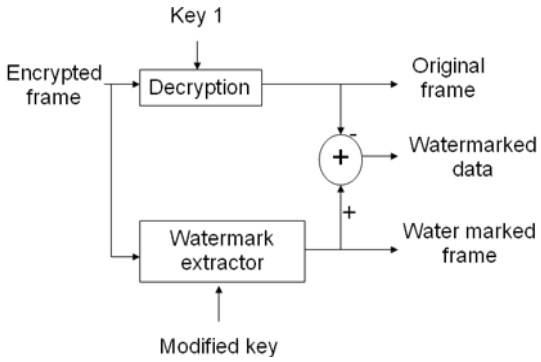


Fig 5 Block diagram for authentication

To do this we need the original frame without watermark. This frame can be extracted at the receiver side using the original key used for encryption, which was available only to the owner of the video. The encrypted frame was available at the receiver side from this we can find the original frame using,

$R_{ij}=R'_{ij}$ XOR K_{ij}
$G_{ij}=G'_{ij}$ XOR K_{ij}
$B_{ij}=B'_{ij}$ XOR K_{ij}
Where,
R_{ij}, G_{ij}, B_{ij} →Original Frame.
K_{ijr}, K_{ijg}, K_{ijb} →Keys for Encryption.
R'_{ij}, G'_{ij}, B'_{ij} →Encrypted Frame.

The watermarked frame can be obtained by using the encrypted frame and the modified key using

$W_fR_{ij}=M_{ij}$ xor R'_{ij}
$W_fG_{ij}=M_{ij}$ xor G'_{ij}
$W_fB_{ij}=M_{ij}$ xor B'_{ij}
Where,
M_{ijr}, M_{jg}, M_{ijb} →Modified Keys
R'_{ij}, G'_{ij}, B'_{ij} →Encrypted Frame
W_fRij, W_fGij, W_fBij →watermarked frame.

So, just by subtracting the original frame with watermarked frame we can get the watermarked data.

$Nr= W_fR_{ij} - R_{ij}$
$Ng= W_fG_{ij} - G_{ij}$
$Nb= W_fB_{ij} - B_{ij}$
Where,
W_fR_{ij}, W_fG_{ij}, W_fB_{ij} →Watermarked frame.
R_{ij}, G_{ij}, B_{ij} →Original Frame.
N_r, N_g, N_b →Watermark Strength.

By this we can obtain the watermark data inserted for a specific user and the authenticity of the user was checked.

V. RESULT

A. Subjective Analysis

(1) Haze Removal on Image and Video

In this section we performed the dehazing for an image and video coding. The input image and video are in the form of haze. Haze is the atmospheric phenomenon. It reduced the quality of image/video. Image and video dehazing is an important problem of common concern in image processing and computer vision areas. Recently, most researchers have adopted physical model based image dehazing to remove haze, where haze is an atmospheric phenomenon such as dust, smoke and other dry particles obscure the clarity of the sky. So the dehazing is necessary for hazy images and videos.

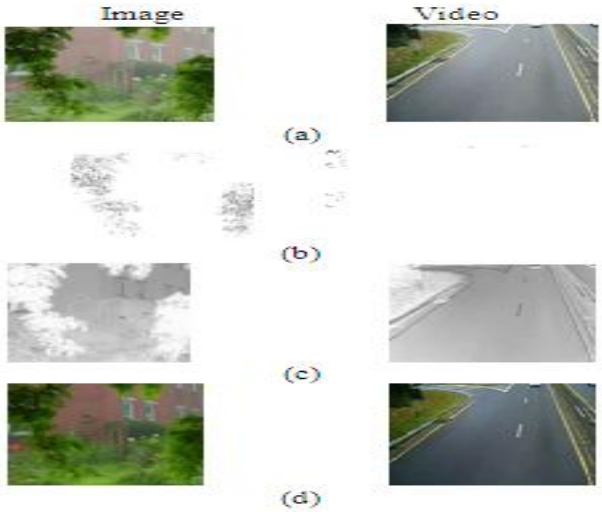


Fig 6 Dehazing effects on Image and Video, (a) Original Haze image and Video, (b) Dehazed using DCP method, (c) Dehazed using MDCP method (d) Output Dehazed Image.

(2) Secure Remote Surveillance System

In this section we performed the secure remote surveillance system. In that the encryption, decryption and key code watermarking operations were performed. The subjective results are shown in fig 7.

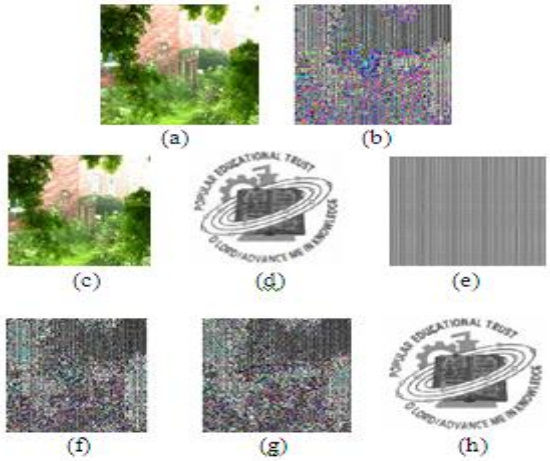
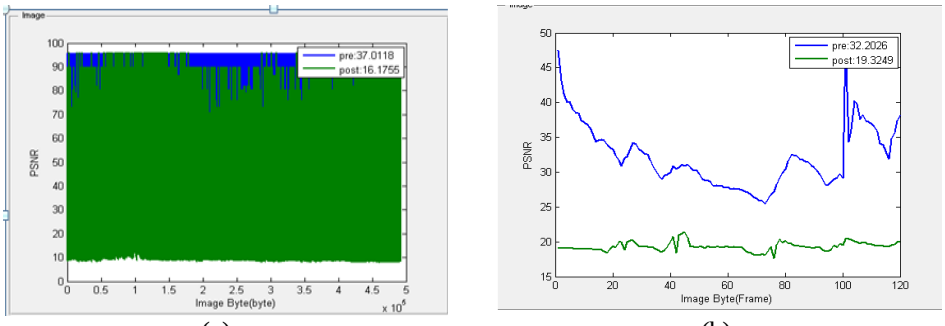


Fig 7 Secured system, (a) Original Image, (b) Encryption before Watermark, (c) Watermarked Image, (d) Watermark to be inserted, (e) Encryption after Watermark (Modified key), (f) Decrypted Image, (g) Decrypted Watermark Image, (h) Watermark Extracted

***B.* Objective Analysis**

In this section the objective measures was performed and the PSNR for the image and video was calculated and represented in graphical form.



(a) (b)

Fig 8 Objective analysis, (a) PSNR of Dehazed Image, (b) PSNR of Dehazed Video

VI. CONCLUSION

The dehazing performance for image and video coding system was discussed to decide Pre or Post method for enhancing and compressing video for a surveillance application where fog and haze are prevalent in the atmosphere. Then the proposed dehazing method produced very few artifacts, fast and better performance for image when JPEG compression and video coding method when H.264 video sequences is used. Then the simulated results confirmed the analysis. In next phase, the concept of watermark and encryption were added to this dehazed image and video for digital right management, by using a fast and reliable light weight algorithm. Finally the image and video can be used to trace illegal distribution. Thus the resulting system produces a dehazed image and video with high security and fast transmission.

VII. ACKNOWLEDGMENT

I have taken efforts in this paper. However, it would not have been possible without the kind support and help of many individuals. I would like to extend my sincere thanks to all of them. I am highly indebted to Mrs.S.I.Padma for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the paper. I owe a sincere prayer to the LORD ALMIGHTY for his kind blessings and giving me full support to do this work, without which would have not been possible. My thanks and appreciations also go to my colleague in developing the paper and people who have willingly helped me out with their abilities.

REFERENCES

[1] Agi.I and Gong.L, (1996) "An empirical study of secure MPEG video transmission" in Processing of Symposium., pp. 137-144.

[2] Chaudhry.A, Iqbal.K, Khan.A and Mirza.A, (2006) "Enhancing Contrast of Compressed Images: Reducing Block Artifacts Adaptively" .Piscataway, NJ: IEEE Press, pp. 140-145.

[3] Chen.Z, Abidi.B.R, Page.D.L and Abidim.A, (2006) "Gray-level grouping (GLG): "An automatic method for optimized image contrast enhancement- part I: the basic Method", IEEE Trans. Image Process., vol.1, no.8, Pp. 302- 2290.

[4] Chen.Z, Abidi.B.R. R, Page.D.L, and Abidim.A, (2006) "Gray-level grouping (GLG):"An automatic method for optimized image contrast enhancement- part II: the Variations", IEEE Trans.Image Process., vol 15, no.8, pp. 2303-2314.

[5] EuijinChoo, Jehyun Lee, Heejo Le and Giwon Nam, (2007|) "SRMT light- weight Encryption scheme for secure real time multimedia transmission".MUE'07.International Conference, Pp 60 – 65.

[6] He.K, (2009) "Single image haze removal using dark channel prior," in proc.IEEE Conf.ComputVis.PattrernRecognit, Pp 1956-1963.

[7] Jain.J and Jain.A, (1981), "Displacement measurement and its application in interframe Image coding, IEEE Trans. Commun" vol.29, no.12, pp 1799-1808.

[8] Kanjanarin.W and Amornrasaka.T (2001), "Scrambling and key distribution scheme for Digital television". Preceding the ninth IEEE International conference, pp 140- 145.

[9] Leow.M, (2003), Closed-form quality for compressed medical images: Statistical preliminaries for transform coding," in Proc. 25th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc., pp 837-840.

[10] Lintian Qiao, Nahhrstedt.K, and Ming-Chit Tam (1997). "Is MPEG encryption by using random instead of zigzag order secure?" Proceeding of 1997 IEEE International symposium, pp 226-229.

[11] Liu.S, Zou Ling Ling, Xie Changsheng, and Huang Hao, (2006), "Two way selective encryption algorithm for MPEG video". IWNAS '06, International Workshop.

[12] Bovik.A, (2002), "Efficient DCT-domain blind measurement and reduction of blocking artifacts," IEEE Trans. Circuits Syst. Video Technol., vol.12, no.12, pp.

[13] Vo.D, Nguyen.T, Yea.S and Vetro.A, (2009). "Adaptive fuzzy filtering for artifact reduction in compressed images and videos", IEEE Trans. Image Process., vol. 18, no.6, pp 1166-1178.

[14] Wang.S, Lin.T and Lee.C, (2005), "New motion compensation designs for H.264/AVC decoder", in Proc. IEEE ISCAS, pp 4558-4561.

[15] Wiegnd.T, Sullivan.G, Bjontegaard.G and Luthra.A, (2003), "Overview of the H.264/AVC video coding standard", IEEE Trans. Circuits Syst. Video Technol., vol.13, no.7, pp 560-576.

[16] Xingyong L, Weibin Chen, I.Shen, (2010), "Real time dehazing for image and video", 2010 18th Pacific Conference, pp 62-69.