Securing Videos using Selective Encryption and Watermarking using HAAR

Anchal Monga
Dept. of CSE
Uttarakhand Technical University, Dehradun, India

Anubhooti Papola
Dept. of CSE
Uttarakhand Technical University, Dehradun, India

ABSTRACT
Demand for videos has grown many folds in the recent past. They can be used for many purposes ranging from educational purposes to entertainment. With the demand comes the fear of the videos being misused or tempered with and the authors denied of the income as the pirated videos can go viral. In the previous researches, watermarking is viewed as the solution for the problem of securing videos. Watermarking is a process of entrenching hidden signals into the data being transferred. The security of videos in present days becomes the key issue in the field of technology and research. Due to the day by day increase in the number of cases of piracy and cloning, the need of more secure and robust system arises. This work focuses on the need of securing videos for different purposes which can broaden its services. The proposed method (SVSEWH) focuses on selective selection based on costing and prime numbers. The videos are first read frame by frame the features of frames are stored and costing calculated with the previous frame. The encryption applied here is the selective encryption in which improvised genetic algorithm is used. The frames qualifying the costing criterion are encrypted using an improvised genetic algorithm and then the prime frames qualifying as prime numbers are watermarked using HAAR transformation.

Keywords
Selective Encryption, Watermarking, HAAR Algorithm, Video Encryption.

1. INTRODUCTION
Nowadays video streaming services is becoming trendy as different variety of media data, such as news, entertainment and instructional contents are widely available to users. Video users are surely thrilled with such convenient services over the network, even if they may also pay subscription fees for commercial contents of videos. Productive markets with new business models of video streaming services for this motive can be created. However, the effect of the illegal distribution of copyrighted videos is raised, which keeps the content owners/creators from adapting the technology of video streaming, and will restrict its range of application. Digital Rights Management (DRM) is observed as a significant mechanism to preserve the exclusive rights of videos and make sure the applicability of video streaming. DRM can encrypt and guard video contents by using cryptographic techniques before the transfer. The authority of conditional access is permitted to legal recipients with decryption keys for decoding videos to watch at the receiver's end. Nevertheless, if some recipients misuse the policies maliciously, the subscribed content could be changed intentionally and redistribute without any control. Digital watermarking is proposed as a cure for this problem in DRM. A digital watermark is an undetectable signal placed into the multimedia data carrying the important details related to owner or data. Since the digital watermark is inserted and fixed carefully with the digital media, it can provide a protection when the cryptographic tool of DRM fails. One important function of digital watermarking is to track which recipient illegally redistributes the copyrighted data. A feasible situation is described as follows. Before transferring a video to the legal recipient, the content's owner inserts the characteristics of the recipient into the video file as the watermark. The watermark is detectable to the recipients since it is inserted in an undetectable way complying with the human perceptual system. The watermark can be acknowledged by using computing devices, and the records of it can be extracted to differentiate between the varieties of users. The inserted watermark is tough to be removed and should oppose data-preserving video processing, such as transcoding, geometrical transformations of frames, and temporal alteration, etc. Once an illegal replica is found on the Internet, a special watermark can be identified from it to definitely find the source of unauthorized sharing. This approach can threaten recipients' objective of distribution of data around if they are familiar with such methods. Since digital videos are usually compressed before transfer, it is preferable to apply digital watermarking to the compressed video streams directly. Some issues still exists in the system, the issues are as follows. First, many existing techniques are created to function with the raw video frames, but the accessibility of which may create trouble in streaming services. Most video owners of course treasure their raw contents very much, and they are continually reluctant to give away the precious raw data to the streaming services, let alone the impractically large size of volume. Moreover, in such applications, each video for a particular recipient will be inserted with a special watermark, and therefore each video has to be programmed and process separately. The computational load of video server will be elevated severely in comparison to the range of recipients. Although it may be possible to transfer this mission load from servers to recipient, complexity is still a concern as the recipients is generally a resource constrained tool due to the cost problem. Supplementary loads caused by watermark insertion could greatly influence routine operations of video processing and interpretation at the recipient. Inserting the watermark completely into the compressed bit-stream is definitely a further promising strategy to control server complexity. However, it needs more alert and tricky designs, given the certainty that the problems about robustness and potential of watermarking in compressed videos are very difficult. Various watermarking scheme are earlier proposed to prevent the content of digital data but they are futile to meet the conditions of security of the digital contents. So there is the need of more protected system for a transmission of videos so that the unauthorized user cannot access the contents of video. For that purpose watermarking can moreover be associated with additional digital image processing techniques such as encryption. Encryption is a method to convert original data into the encoded data. Encryption is an operative way for the

transmission of multimedia data over the web. In this system the watermarking alone is not able to protecting the contents of video data so the watermarking is joined with the encryption to make the more robust system.

2. LITERATURE REVIEW

Po-Chyi Su et al. (2017) in their work [1] proposed a realistic design of digital watermark for video services. The data of legal receiver is offered as a watermark, which is embedding in the video stream to present a signal to trace the receiver in case a copy of the video is not lawfully distributed. The watermark signals are crafted to insert in some portion of video frames to help the video stream server, as the result of only partial actions required, including decoding, processing and re-encoding. The invariance of feature point and the self-similarity of concealed signals are more exploited to facilitate watermark detection exclusive of relating to the original video. The watermark can graciously endure transcoding processes and geometrical modifications of frames. The experimental results reveal the merits of the proposed scheme in conditions of watermark detectibility, capability and recognition methodology.

Rupali N. Hole et al. (2017) in their paper [2] proposed a selective encryption system for the protection of video data. The main motive is to advance the safety of data being transferred i.e. to elevate the strength of the video data.

Babatunde A.N. et al. (2017) in their paper [3] depicted a survey of various existing encryption methods with the particulars of the scheme of video compression. The overview of which investigate the performance metrics used in the estimation and evaluation of the exertion of video encryption techniques which offers an overview of a variety of encryption methods.

Ashrith K.A et al. (2016) in their work [4] presented an overview of diverse video encryption techniques. Encryption is broadly used method which offer safety for video transfer and thus various encryption techniques are presented. In this work, the various video encryption techniques and contrast among encryption methods are presented. With respect to not only their encryption rate but also their safety intensity and streaming size. In this research, video stream quality and variety of the best encryption technique is depicted.

Ms. Mahua Pal et al. (2016) in their paper [5] presented the survey on different watermarking schemes. They explained that digital communication plays a very imperative task in our day to day life on the web as well as in other communication technology. The privacy of the information we are sharing is an essential part. One perceptible method is digital watermark. The copyright owner finds out techniques to manage and identify the secrecy of the scheme.

Palwinder Singh et al. (2016) in their paper [6] presented a wavelet transform which is one of the most dominant theory in image processing. Wavelet transformation splits the given function into various scale components and can reveal the frequency information without losing the temporal information. Wavelet transformation is most appropriate method in comparison of Fourier transformation as it is not feasible with Fourier transformation to monitor changing frequencies with time. Image processing is a mechanism, by which we can process digital images which include number of steps like denoising, segmentation, compression, representation and recognition. This research introduces the concept of wavelet transformation and application of wavelet transformation in image denoising, image segmentation and image compression.

Shaohui Liu et al. (2015) in their paper [7] proposed a real time video watermark technique for MPEG standard where first utilizes fast scene segmentation to the real video string and adaptively chooses suitable scenes to be inserted. Further, visual model is exploited to altered watermark strength. Watermark are strength by regulated the no. of bit1 in bitstreams through changing standards of run-level pairs. An experimental result depicts little loss of video quality and also displays excellent robustness against many attacks. As watermark is directly identified in bitstreams domain, real-time exposure becomes a reality. In addition, the embedding policy assures that the bit rate is not improved and the experiments also approve it.

Ankita Sharma et al. (2015) in their paper [8] presented a digital watermarking method is applied for securing data from illegal distribution of information. It is an art of concealing digital information such that unauthorized user can not access or create a replica of data for exploitation. Data which is embedded into the digital media is known as the watermark. It is basically information about the records. The proposed scheme is an evaluation about the improvements in digital watermarking schemes in both the spatial and transform domain.

Lalit kumar Saini et al. (2014) in their paper [9] gives a complete overview of all watermarking methods particularly aims on image watermarking and their applications. They also explains that digital media is essential for today's world as the replacement of paper media. As the technology grows digital media needs security while transmission over the internet. Watermarking schemes are created to accomplish this need.

Jolly Shah et al. (2011) in their paper [10] presented a research in which categorization and explanation of different video encryption techniques are discussed. Study and illustration of various algorithms with respect to different parameters like encryption ratio, speed, cryptographic security etc are explained. The encryption techniques are developed to protect text data are not appropriate for multimedia applications due to huge amount of data and real time constraints.

Salah Aly et al. (2009) in their paper [11] proposed a scheme in which AES can be used for protecting real time video transfer with light processing overhead over the internet. The research shows the comparison between AES and XOR encryption algorithms with normal transmission.

A.Massoudi et al. (2008) in their paper [12] proposed an overview of selective encryption techniques for images and videos security. In this only some part of the data is encoded. The primary agenda of selective encryption is to minimize the extent of data to be encrypted while sustaining the required level of safety. Additionally selective encryption maintains the scalability of the system. This research presents an overview of different selective encryption techniques. The historical background, applications, challenges and perspective is depicted.

Adnan M. Alatter et al. (1999) in their paper [33] presents three new selective encryption methods for safe transfer of MPEG-1 bit streams. These methods preserve higher security standards than earlier presented selective encryption methods while keeping reasonable processing time. In the first process, the encryption is applied to the data allied with each nth I-macroblock. In the second process, the encryption is applied

to the headers of all the predicted macroblock as well as the data linked with every nth I-macroblock. In the third technique, encryption is applied to every nth I-macroblock as well as to the header of every nth predicted macroblock. In the last technique, with n=2, is found to be more effective out of the three presented techniques. This technique accomplishes 60-82% decline in the processing time over total encryption and the simulation result illustrates that the encoded video is fully concealed.

Whitefield Diffie et al. (1976) in their paper [41] examined two different kinds of current progresses in cryptography. Extended applications of teleprocessing, given rise to the requirement of new kind of cryptographic systems, which diminishes the requirement for secure key distribution channels and provide the equivalent written signature. It recommends different ways to resolve these currently open issues. It also explains how the theories of computation and communication are offering tools to resolve cryptographic problems.

3. RESEARCH METHODOLOGY

The algorithm of the presented work is as follows:

SVSEWH Algorithm:

Setup

Initialize required variable

Define costing function

Costing ← a random minima between 0 and 0.25

Working

Step1. Initiate video codec

Step2. Select a video file

Step3. Frame0← read first frame

Sf0← get sift features of Frame0

Step4. Loop from second frame through the video

Step5. Frame i← read video

Sfi←get sift features of frame i

Cost ←

$$\frac{\left(\left|median(\,frame0) - median(\,framei)\,\right|\right)}{\left(\max(\,frame0) + \max(\,framei)\right)}$$

Step6. If Cost<costing then

Step7. Encrypt frame using algo 1.1 // Encryption applied here

Sf0 ←sfi

Step8. End

Step9. if prime frame then

Step10.Watermark the frame using algo 1.2 //Watermarking applied here

Step11.End if

Step12.End loop

Algo.1.1. Encryption // Encryption (Step: 7)

L=64

// pre-process //

Loop i till number of channels

Loop j till number of rows

Loop k till number of columns

R_{n1}← $-j^{(j+k)}$

$R_{n2} = -i^{(j+k+1)}$

$R1_{ijk}$←I_{jki}/256 *L

$R2_{ijk}$←I_{jki} /256 *L

$xx_{j,k,i}$←I_{jki} /256 *L

$R1_{jki}$← R_{n1} X $R1_{jki-}$

$R2_{jki}$← R2n*$R2_{jki}$

end

end

end

//Modified-Mutation with Crossover//

Loop i till number of channels

Loop j till number of rows

Loop k till number of columns

k1← k*rand() %random generation

j1← j*rand()

if k1>0 and j1>0 then

key_{jki}← 255-key_{jki}

x_{jki}← y_{j1k1i}

$v1_{jki}$← 255 - x_{j1k1i}

otherwise

x_{jki}←y_{jki}

$v1_{jki}$← 255 - x_{jki}

key_{jki}← 255-key_{jki}

end

end

end

end

//further manipulation//

Loop i till number of channels

Loop j till number of rows

Loop k till number of columns

$v1_{jki}$← 255-$v1_{jki}$

key_{jki}← 255-key_{jki}

if $v1_{jki}$ NOT equal to key_{jki}

$v1_{jki}$ = key_{jki} X 256/64 //Encrypted value for the frame

end

end

end

end

Algo.1. 2. Watermark //Watermarking (Step: 10)

Step1. Perform haar based dwt on the frame

Step2. Extract red, green and blue channels of the frame

Step3. [U, S, V]←Perform singular value decomposition (svd) on each channel

Step4. U is left singular vector

Step5. S is Singular values Diagonal matrix

Step6. V is right singular vector

Step7. Perform haar based dwt on the image to be watermarked

Step8. Repeat steps 2 through 7

Step9. Multiply USV values of each channel and store in variables

Step10.Concatenate the values generated in 9 to form an image

Step11.watermarked Image←perform inverse wavelet on matrix generated in 10

The working of the SVSEWH algorithm can be explained as firstly we have to initialize the video codec for start the processing on video file. Then we have to select the video file which can be in any format like MP4, AVI, HD etc to starts the processing of the system. Now the video start processing and we can read the frames of the video. Read the first frame of the video and get the SIFT features of the first frame to start the process of encryption. The encryption applied here is a selective encryption where only some frames of the video are encrypted which made the video easy to transfer over the network without making it heavy. The algorithm applied in a selective encryption is modified genetic algorithm. The genetic algorithm works on a concept of mutation and crossover. After the application of processing on the first frame, the frame i is read and we have to get the SIFT features of the frame i. The basis of selection of frame is cost. if the cost is less than costing then the frame is selected and then we apply the encryption algorithm 1.1 here and start executing it. And then we check the frame number of the video file, if the frame number of the video is prime then we apply the watermarking algorithm 1.2 here. If the frame number is non prime then we again check the frame number until we get the prime number frame.

In the encryption algorithm 1.1, the processing of the system is started after the calculation of costing function. If the cost is less than costing then the encryption started in that frame. The L value is supposed to be 64, where L value is any random value. Then the set of certain conditions is checked and keys are applied in this step for the further processing if the conditions satisfied then we perform mutation and crossover on the frame to get the matrix and then we check if the matrix end. If it is yes then subtract 255 from each element of the matrix after the application of mutation and crossover. Then we get the encrypted frame. After that the processing of the system ends.

In algo.1.2. Watermark, firstly we have to select the prime number frames. Then we apply HAAR based DWT on each frame that we satisfied the criteria of prime number. Now we have to extract red, green and blue channels to the frame to start the processing of watermark. Then do a singular value decomposition on each channel which is define in the form on U, S, V where U indicates left singular vector, S indicates singular value diagonal matrix and V is the right singular vector. Next perform a HAAR based DWT on the image which have to be watermarked. Repeat the above steps till the end of the all channels of the frame. Then multiply the USV values of each channel and store in the variables. Concatenate the value generated above to form an image. For getting the watermarked image we have to perform an inverse wavelet transform on the matrix.

4. RESULT AND ANALYSIS

When the system starts processing, firstly the encryption works then the watermarking is applied. In the encryption process, the selective encryption is applied in which only some frames are encrypted not all. The encryption is applied by firstly selecting a particular frame then divides the frame into R, G and B channels then the preprocessing is applied and generates a matrix in which a random value is added to the pixels and the key is generated. The frame is encrypted now. After that the watermarking is applied, the criterion for the selection of frame for watermarking is that the frame should be a prime number frame. The frame is selected then the features of the frame is extracted after that we applied a HAAR based on discrete wavelet transform. The quality of the image or video extracted is same as the original video so the scheme is very efficient as compared to the DCT-SIFT scheme. For the decryption, we applied an inverse DWT in the system and watermark can be detected by extracting the images from the videos.

The details of the simulation carried out on the system in shown here.

It is tested on the video named analysis (150 frames) in the video format of .avi with the resolution of 640x480 and the total bit rate is 8838 kbps.

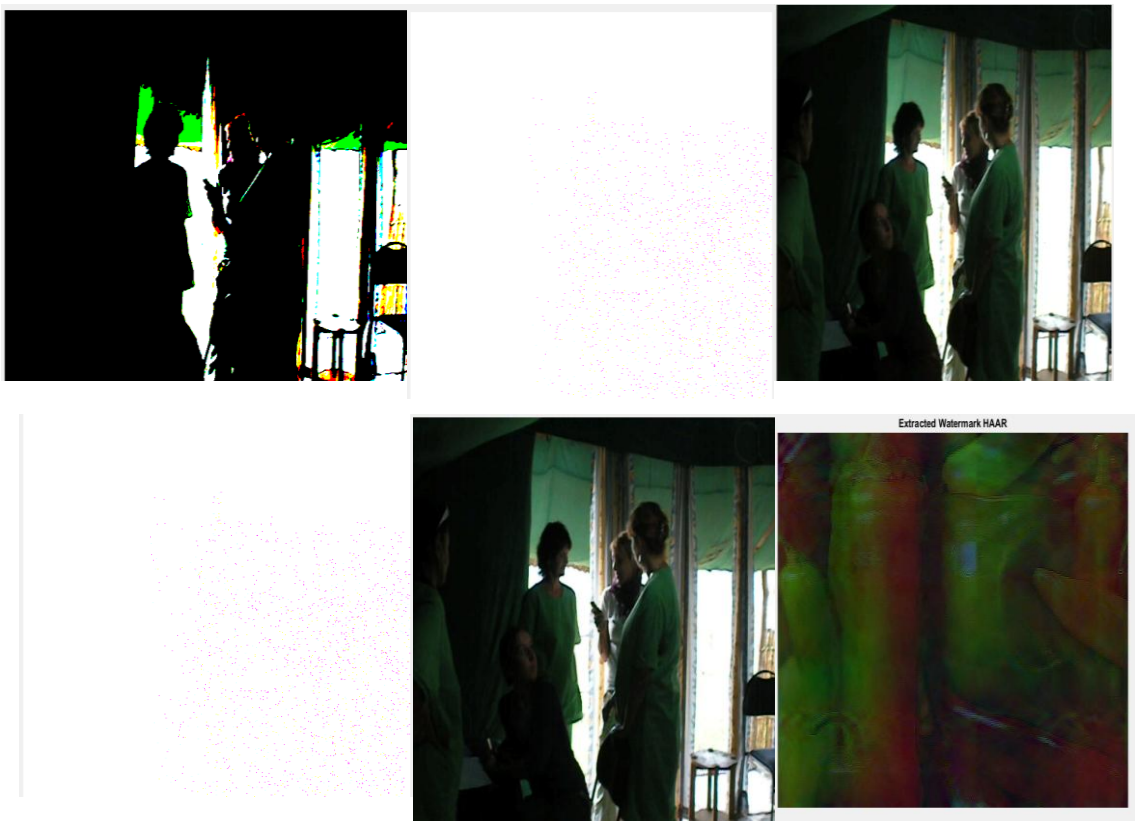

Fig.1: Still images of the SVSEWH system.

The resultant description of the scheme is shown in the figures which are captured during the system runs. The still images are captured and shown. The quality of the captured still images is same as the video quality of the input video.

Four Error metrics are used to compare the various image encryption techniques are the: Mean Square Error (MSE) , NPCR (Number of Changing Pixel Rate), UACI (Unified Average Changing Intensity) and the Peak Signal to Noise Ratio (PSNR).

The MSE is the cumulative squared error between the encrypted and the original image.

PSNR is a measure of the peak error.

PSNR= 20*log10 (255/sqrt (MSE)

A low value of MSE means less error and there is an inverse relation between the MSE and PSNR, this translates to a higher value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the signal is the original image and the noise is the error in reconstruction of the image. So, if you find a compression scheme having a lower MSE (and higher PSNR), you can find that it is a better one.

The results shows that the value of error matrix, PSNR is increased by approximately 7% and the values of MSE is about 51% of the base scheme which shows that the result are good as compared to the base scheme. The value of NPCR and UACI is also higher from the base scheme. So the proposed scheme is more effective in video encryption and can be applied for video encryption in different fields which requires the high level of security. The graphs of the proposed SVSEWH scheme are shown below:

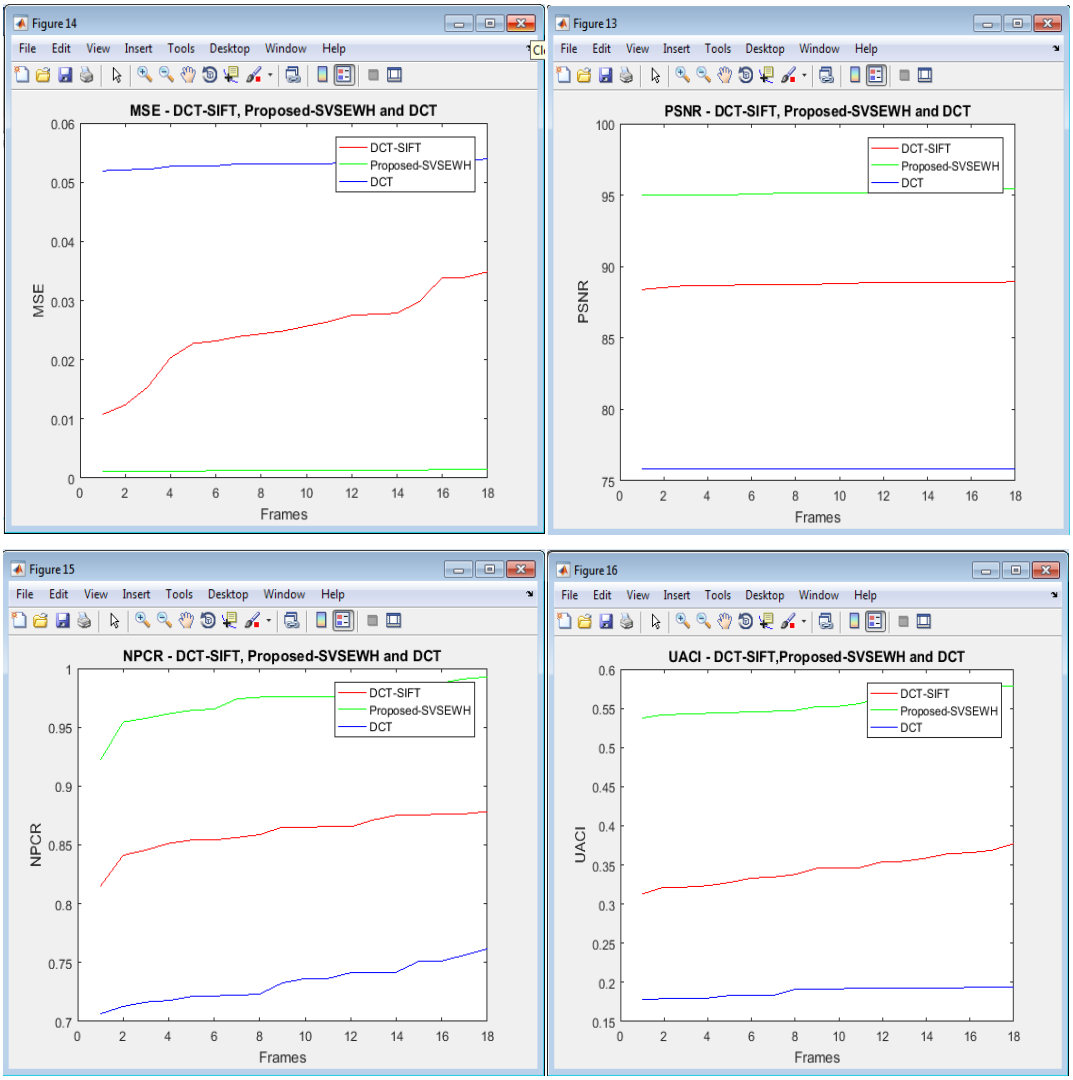

Fig 2: Graphs of Comparison of DCT-SIFT, SVSEWH and DCT Schemes.

5. CONCLUSION

The thesis presented an idea of making more effective and reliable video security scheme. In this thesis encryption of the frames is presented by using a selective encryption technique which aims at the increases the overall security of the system on the basis of costing. Watermarking on the selected frames can be performed by the criteria of prime numbers that means that if the frame is prime number frame then the watermarking is applied. They together make the system more robust and avoid different types of attacks like Gaussian filtering and rotational attacks. The results shows that the values of error matrix, PSNR is increased by approximately 7% of the base scheme , the values of MSE is about 51% of the base scheme, the values of NPCR is greater than the base scheme and the values of the UACI is also greater than the base scheme. So, the proposed scheme is more efficient than the base scheme and it can be applied for the schemes which required higher level of security. It can also be observed that it is free from different types of attacks so the manipulation of the contents is not an easy task for the hackers, so the risk of the data fraud is also eliminated and it also have a copyright patent so the hacker also don't misuse the gathered information since it is registered on someone's identity. So from the perspective of security and efficiency it can be applied to the critical fields without any disputes

6. REFERENCES

[1] Po-Chyi-Su, Tien-Ying Kuo, Meng-Huan Li "A Practical Design of Digital Watermarking for Video Streaming Services", Elsevier, volume 42,January 2017, Pages 161-172

[2] Rupali N. Hole, Megha Kolhekar "Robust Video Encryption and Decryption using Selective Encryption" IEEE,2017

[3] Babatunde A.N, Jimoh, R.G, Abikoye O.C & Isiaka B. Y "Survey of Video Encryption Algorithms", CJICT *Vol. 5 No. 1, June, 2017.*

[4] Ashrith K.A, Prajwal S Patil, Raunak Matai, Saurabh Rajpal, Syed Akram "A survey on Efficient and Secure Video Encryption Techniques", IJIET Volume 6, 4 April 2016.

[5] Ms. Mahua Pal "A Survey on Digital Watermarking and its Application", IJACSA, VOL.7, No.1, 2016.

[6] Palwinder Singh" Wavelet Transform in Image Processing: Denoising, Segmentation and Compression of Digital Images" IJSRSET ,Volume 2, Issue 2, 2016.

[7] Shaohui Liu, Daniel BO-Wei Chen, Long Gong, Wen Ji, Sanghyun Seo "A Real-Time Video Watermarking Algorithm for Authentication of Small-Business Wireless Surveillance Networks", IJDSN volume 2015,

[8] Ankita Sharma, Sarika khandelwal "A Brief Introduction to Digital Watermarking", IJCSIT Vol.6 (3),2015.

[9] Lalit kumar Saini "A Survey of Digital Watermarking Techniques and its Applications", Volume 2 Issue 3, June 2014.

[10] Palwinder Singh**"** Wavelet Transform in Image Processing: Denoising, Segmentation and Compression of Digital Images**"** IJSRSET ,Volume 2, Issue 2, 2016

[11] Jolly shah,Dr. Vikas Saxena **"**Video Encryption- A Survey**",** IJCSI vol. 8, Issue 2, March 2011.

[12] Salah Aly "A Light Weight Encrypting for Real Time Video Transmission", 2009

[13] A.Massoudi "Overview on Selective Encryption of Image and Video: Challenges and Perspectives", Springer, Volume 2008, January 2008 , Article No. 5, 2008.

[14] Adnan M. Alatter "Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-Streams", IEEE vol.48, No.4, November 2002.

[15] Whitefield Diffie "New Directions in Cryptography", IEEE, Vol-IT 22, No.2, November 1976.