The Journal of Research on the Lepidoptera Volume 51 (1): 783-792
The Lepidoptera Research Foundation. March 2020
ISSN 0022-4324 (print) ISSN 2156-5457 (online)

Implementation of Real and Accurate Watermarking System For Security Using Logistic Regression Machine Learning Techniques

DR.B. SANKARA BABU[1], A. SAMPATH DAKSHINA MURTHY[2], SAMPENGA VEERRAJU[3], B. OMKAR LAKSHMI JAGAN[4] AND K. SAIKUMAR[5]

[1]*Professor, Department of Computer Science Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India.*

[2]*Assistant Professor, Department of Electronics and Communication Engineering, Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, A.P, India.*

[3]*Department of Electronics and Communication Engineering, Vignan's Institute of Information Technology (A), Visakhapatnam, A.P, India.*

[4]*Research Scholar, Department of Electrical and Electronics Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India.*

[5]*Research Scholar, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India.*

[1]*bsankarababu81@gmail.com,* [2]*sampathdakshinamurthy@gmail.com,* [3]*veerraju.s@gmail.com,* [4]*omkarjagan@ieee.org,* [5]*saikumarkayam4@ieee.org*

Abstract.
Technology overgrowing from the 20th century, nations like developing countries needs the authorization of multimedia applications for defence, navy and military applications. The defence academies, satellite, radar organizations like DRDO, ISRO, and HAL requires confidential data sharing applications. The multimedia applications using image and videos are communicating through different types of channels like wired, internet and broadcasting. Such organizations and academies share this data to all authorized persons, un-authorized users unable to hack this data. The authorized users have utilize this data with the help of encryption and decryption keys. The secrete key is shared to authorized persons (clients) only if any hackers or fraudsters try to hack this information unable to retrieve original data. At this scenario, unauthorized clients did not get confidential files, from the past two decades, the key generation for image and video watermark investigation has been moved rapidly. Different algorithms like genetic algorithm, differential evaluation, conventional methods had been designed for secure transmission and receiving purpose. But, modern technologies overcome this key generation and easily hacking the information. The significant objective is secreted multimedia digital image and confidential video transmission, high hidden capacity data. Accuracy is 97.81%, efficiency is 95.6% and true positive rate 0.96 improved.

Keywords. Watermarking, Logistic Regression, Security, Video and Image.

Received: 08 February 2020
Accepted: 28 February 2020
DOI: 10.36872/LEPI/V51I1/301073

The Journal of Research on the Lepidoptera Volume 51 (1): 783-792
The Lepidoptera Research Foundation. March 2020
ISSN 0022-4324 (print) ISSN 2156-5457 (online)

INTRODUCTION

The image or video sharing techniques and algorithms have been discussed in below literature contains more limitations such that need machine learning and neural networks (deep learning) mechanisms. This chapter briefly explains about different robust digital watermarking algorithms and techniques has been discussed. The quick and accurate extraction of digital multimedia images and video via broadband is an quite different methods. Copyright, watermarking and cryptography is a study to gives a security for third party organizations. Steganography is a concept hide the information in particular manner no one doubts the information existence of message. In cryptography security related to secrete key length but steganography related to different types of cypher information. The digital watermarking on standard resolutions like 512 x 512 image with eight bit grey scale picture authentication information are authorized keys and image interpretation discussed in [1].

In this investigation the capacity of counter fit and controlled access of image regarding digital watermarking had been implemented and discussed in two ways. The first model is based on BPM(Bit plane manipulation) of least significant bit this model offers simple and rapid embedding method. The second model used for linear summation of digital watermark image information, this is more difficult to embedded also offering heterogeneous security. This investigation trains the digital image on feasible image testing but various problems find with summing the digital watermark retain dynamic scale of real image and cross, auto correlation extraction process. This method LSB is difficult to insert a key sequences on compression and digital watermark image processing. The message like “aaa,bbb,ccc,AAA,BBB,CCC” is circumstance encryption key, this technique had been failed for real time, online executions.

RELATED METHODS

Digital data image encryption typically differentiates the encryption and decryption based on security solution had been involved for cryptography technology. The illegal access of multi media images and videos had stop by using digital watermarking technology with this unauthorized operations are privileged. The assumptions can be crack only hackers. At this protection of secure information is approved by digital data image security system in [2&3]. In this a pin pattern has been involved with patent IPN, this situation have some unauthorized access involved such that needs improvement at digital watermarking extraction and embedding process.

The different image formats like JPEG, JPG, PNG, TIFF, MPEG are various techniques used to design an image depending upon pixel nature. Example: static or dynamic pixels. The embedding data information to multimedia (Image or video) termed as watermarking. This is a method increase the attention with respect to authentication and authorization. The real time applications like television broadcasting, video watermarking and video encoding are the topics related to digital watermarking. This scheme is mainly embedding to bit stream of MPEG-two retrieved video decoding. The method watermarking is much lower complex and robust regarding to decoding and encoding pixels of watermarking. An existing methods below MPEG to drift image compensation

has implement confirm the robust digital watermark in[4]. In this securely image has been transmitted with flexible data rates bits/sec, the applicable hybrid encoding schemes H261, H263 and MPEG1 related to copyright© photo optical engineering and instrumentation. This implemented scheme has some disadvantages at extraction process, like pixel loss, less robust, more complex.

The watermark blind embedded extraction and method of video front collection is a model under effective video quality relationship with respect to discrete cosine transform(DCT) coefficients are realize embedded digital watermarking MPEG compression techniques. This implementation related to multimedia video and image applications on different image and video sizes. The copyright protection against security is an attractive model for present watermarking techniques in [5]. This investigation proposes a front video watermark with audio using random blind extraction. In this every frame has been watermark with acquisition of original information related to MPEG compression. Different sizes like images has been transform original image watermark binary technique listed the below sizes.

METHODOLOGY

In current day to day life broadband has become a major transmission and communicated channel for multimedia applications. This prominent prospect has served for digital multimedia organizations. The +ve side increases income of multimedia companies distribution will be infringement over broadband (audio, image and video etc..). This multimedia parameters attracts the investigators to find various methods to come up with different solutions called robust digital watermarking for information sharing. This cheating watermark detection system does not useful for robustness. So, watermark removable models should not allow for better security purpose.

Watermarking is a process embedding significant data of organizations/owners /defence into digital data. The encoding information should be a text/logo/image /sometimes a video which is considered as watermarking. This can be get back from real data when essential to prove it's realization[6]. In general encode a watermark models has posses some significant characteristics such as high capacity embedded system, the excellent maintenance of host media, high robust signal processing attacks like crop, scale, rotation and noise etc.. In some of the situations videos supplementary attacks have possible by averaging the frames, dropping of frames and swapping of frames etc., here attacks can be deserter are malevolent unauthorized users tries to differentiate the/hack watermark information.

Digital watermark block diagram (architecture)

A robust watermark system construct by utilizing the embedded block and extraction block. In this method user/authorized person has to access this content by using cypher information. This cypher keys in the form of video, text, audio and image, the owner can take any type of copyright symbol or logo, fingerprint may be a watermark. During encoding process watermark is introduced to original content at extraction process interleave

watermark is differentiate from original water marked image. The encoding and decoding process as shown in below figures1&2.

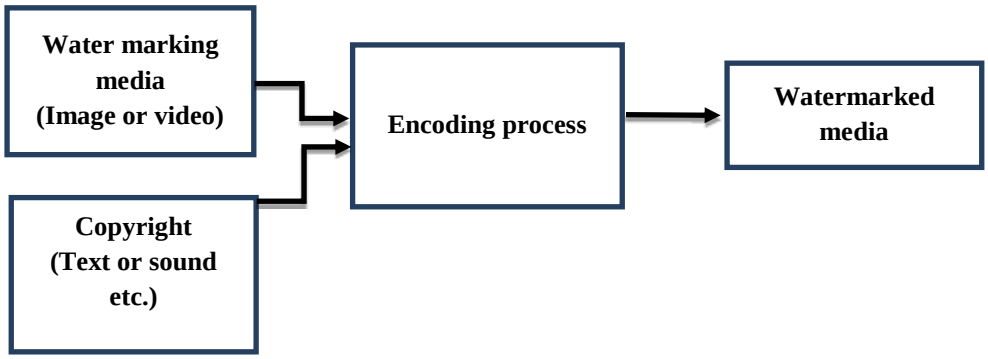

Figure 1. Encoding process

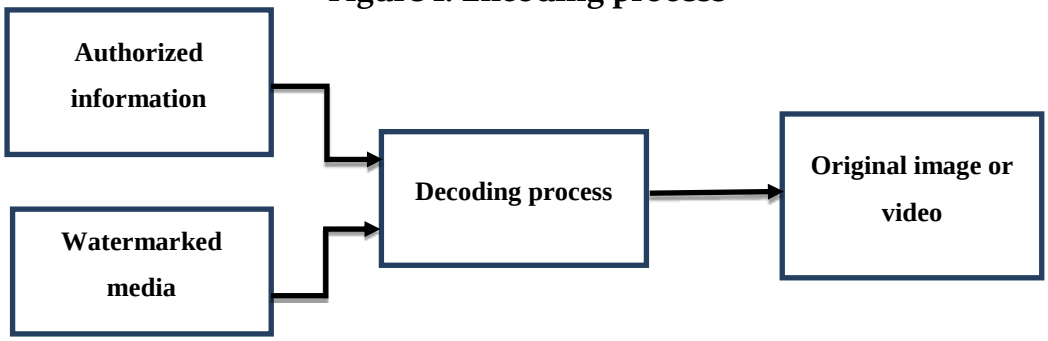

Figure 2. Decoding process

Using watermark extraction and embedding process 64x64 image matrix has been trained with 100 frame video.

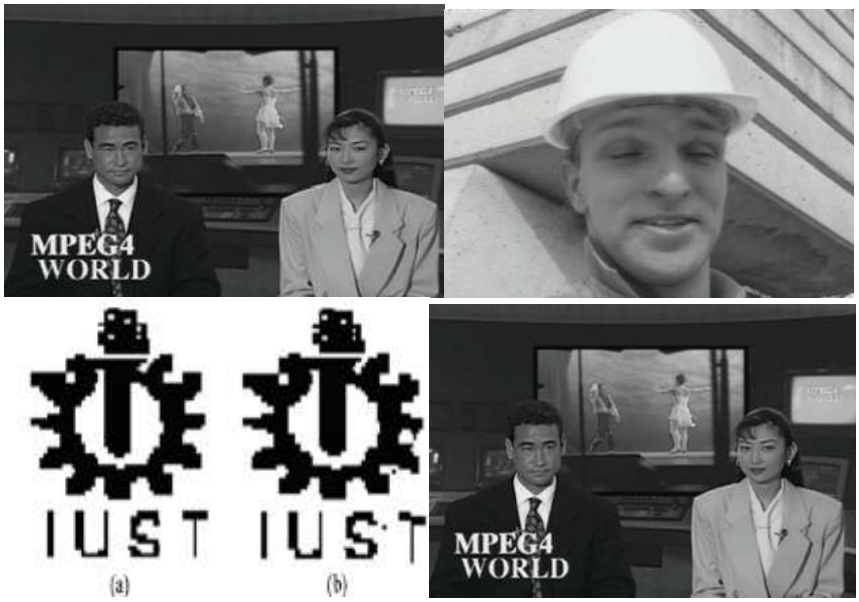

Figure 3. a) The original 100 frame sequence. b) 100 frame sequence original image. c) Extracted and original watermark with NC = 0.9929. d) Watermarked video. (PSNR = ~ 40)

The above fig 3 explains that watermarking procedure by using MJPEG comparison with conventional models[7]. This model gives the better peak to signal noise ratio(PSNR) has been achieved by using below formula1.

$$\text{PSNR} = 20\log\left(\frac{255}{\sqrt{SNR}}\right) \quad (1)$$

$$\widehat{v_i} = \text{argmin}_{-1,1}\left|\left(\frac{v_i}{g(\hat{v}_{-1,1}^{w})}\right) - Q_{bi}\left(\frac{v_i}{g(\hat{v}_{-1,1}^{w})}\right)\right|^2 \quad (2)$$

$$\hat{V}\text{w} = [\widehat{v_1}w, \widehat{v_2}w, \ldots \widehat{v_L}w]. \quad (3)$$

The above equations 2 &3 explains that blind 3D wavelet based watermarking mechanism with this throughput and accuracy is improved. But, attacks are not attained at differential manner.

$$\text{NC} = \frac{\sum_i \sum_j w(i,j) \sum_i \sum_j w^1(i,j)}{\sum_i \sum_j w(i,j)^2} \quad (4)$$

(PSNR = ~ 40). (5)

$$T_h = \frac{\sum_{i=1}^{16} |u_i|^2 - \frac{\left|\sum_{i=1}^{16} u_i\right|^2}{6}}{15} \quad (6)$$

The threshold value th is accepted until frame count that is 16, depends on object rate and video signal. In this method the threshold value is fixed as 40 which are shown in equation 4 to 6 .

The various image dimensions for embedded water marking positions for convenient transmission and size reduction for watermark embedding process. The video compression like MJPEG, MJPEG-X and H-26X is the adopt hybrid extraction related to DCT transformation[8&9]. The watermarking and its extraction against each frame effected the image quality and frequency components at intermediate operations.

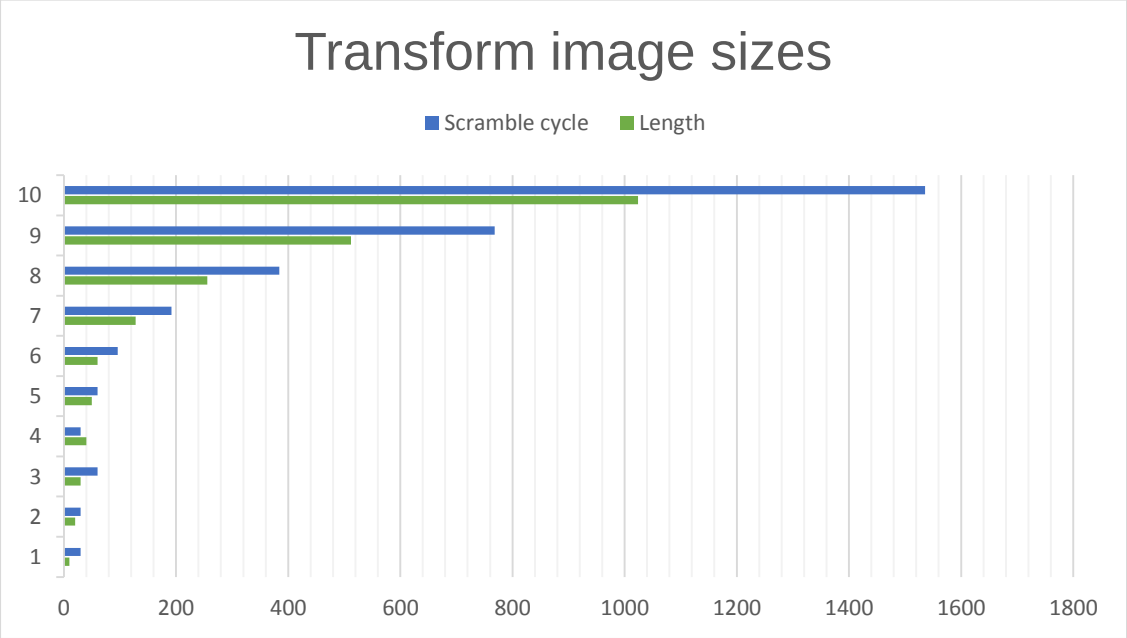

Figure 4. Video embedded position based on image size

The Journal of Research on the Lepidoptera Volume 51 (1): 783-792
The Lepidoptera Research Foundation. March 2020
ISSN 0022-4324 (print) ISSN 2156-5457 (online)

The partial watermark characterized improvement algorithm is developed inbuilt camera captured image size 640x480 video vector frame and watermark image of binary 40x40 process has been allowed. The collection of videos format has been selected as 48x640 with RGB2_4 integrated camera data rate 30FPS and 40x40 image watermark with binary avi uncompressed watermarking is simulated in MATLAB R2009B attain the output.AVI format watermarked videos[10&11]]. This experiment has simulation time is more due to this MJPEG NC value extracted 30 times less efficient compared to modern methods this is the test investigation video explained in fig 4.

Procedure of extraction process

Digital image watermarking technique is found to be very useful for multimedia transmission Digital video watermarking is considered to be one of the efficient processes of sending the information securely.

When W −0, if DCT block DCT block _ (3, 2) _ (2,3) ≤ , the DCT block _ (3,2)

DCT block _ (2,3) are exchanged, and if DCT block DCT block k _ (3, 2) _ (2, 3) Then

DCT block DCT block k _ (3,2) _ (3,2) (/ 2) = + , DCT block DCT block k _ (2,3) _

(2,3)

(/ 2) Others aren't changed. B. When W =1,

If DCT block DCT block _ (3, 2) _ (2,3) > , the DCT block _ (3, 2) and DCT block _

(2,3) are exchanged, and if DCT block DCT block k _ (3, 2) _ (2, 3)

Then DCT block DCT block k _ (3, 2) _ (3,2) (/ 2)

DCT block DCT block k _ (2,3) _ (2,3) (/ 2)

RESULTS

Table 1. HVS method analysis

Attacks	Methodology[10]			Logistic regression method[10]
	Bit error rate(%)			
	Test video 1	Test video 2	Test video 3	Bit error rate(%)
MPEG_2(0.6mbps)	10	14.19	6.23	11.12
Median filter	5.91	3.12	1.13	15.91
Average filter	8.61	7.94	4.75	15.91
wiener filter	16.14	11.89	9.02	15.92
Gaussian	6.74	3.59	4.13	15.91
Salt & papper noise	15.72	3.91	5.79	15.92
Crop	1.82	1.84	1.47	15.92
Translating	21.72	21.71	21.78	15.93
H-flip	19.23	19.23	19.23	15.94
V-flip	21.82	21.87	21.89	15.92
Blur	0.32	0.12	0.21	0.3
Brightness	97.12	9652	97.92	0
Frame Avg	0.34	0	0	0
Frame remove	7.42	0	0	0
Frame swap	0.052	0	0	59.23
Frame substitute	0.83	0.023	0.21	59.23
Frame insert	10	12.91	12.91	59.23
Frame BPr	0.052	0	0	59.23

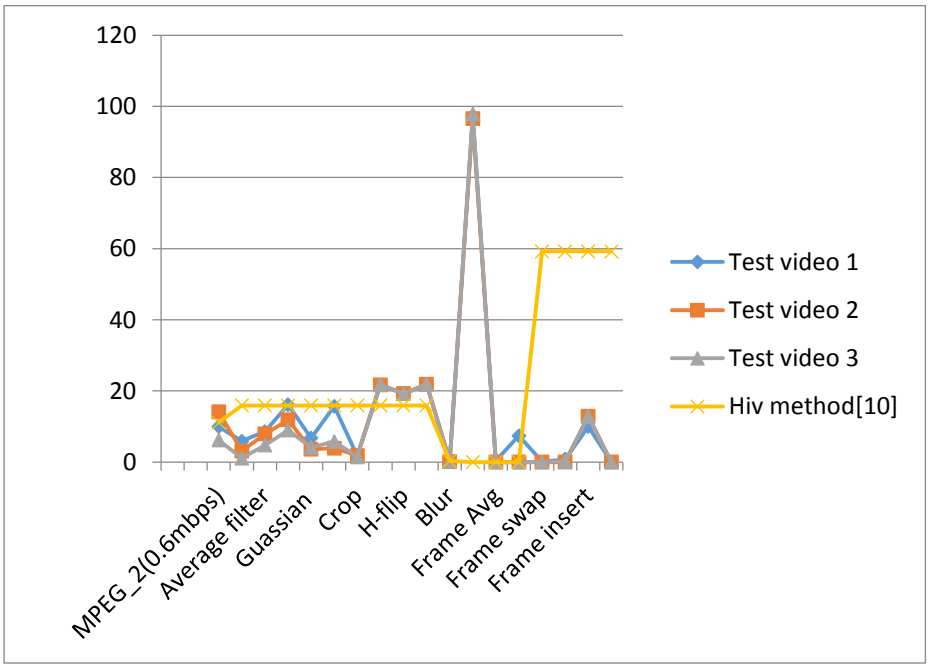

Figure 5. Graphical HVS frame analysis

Fig 5 & table 1 discussion related to test videos and frame rate analysis based on different types of attacks. In this HVS is best digital watermark method but statistical analysis is necessary with neural networks. This can possible only modern deep learning mechanisms.

On the basis of above review, it is found that the most used technique is spatial domain technique because in this the watermark can be easily and successfully recovered if the video is translated or cropped when compared to spatial domain technique.

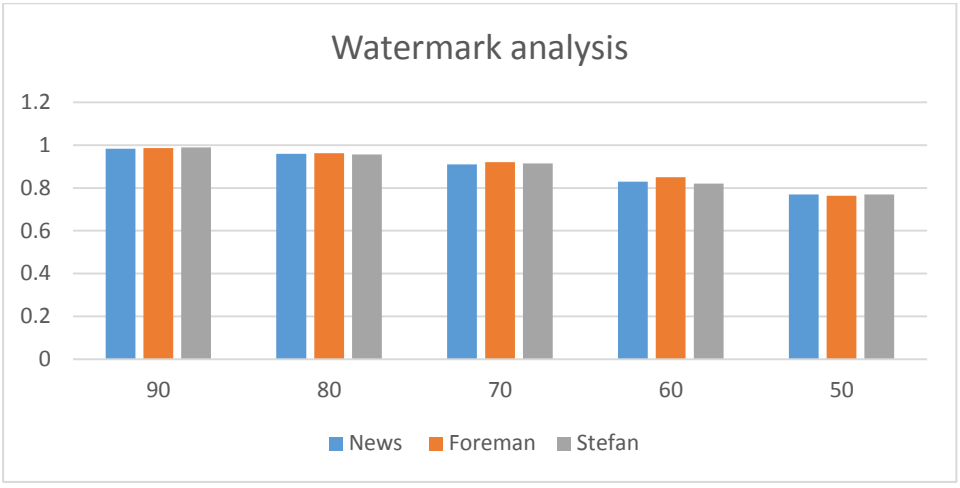

Figure 6. MJEPG watermark analysis

Fig 6 explains that digital watermarking system with respect to 2D-DWT mechanism. In this situation 3 level transformation mechanism has been used to extract the watermarked image with windowing techniques by coefficients. At this stage efficient PSNR is obtained but robustness is required to improve.

The major factor that is taken into consideration while the information is being exchanged over the web is Security. Earlier numerous watermarking strategies have been proposed for the protected information transmission.

Table 2. Frames with respect to attacks

watermark	frame_100	frame_100	water marked
attack free	0.99	0.994	0.98
avg	0.995	0.995	0.992
drop	0.94	9 0.94	0.97
swap	0.96	0.967	0.98
MPEG_2	0.88	0.89	0.89

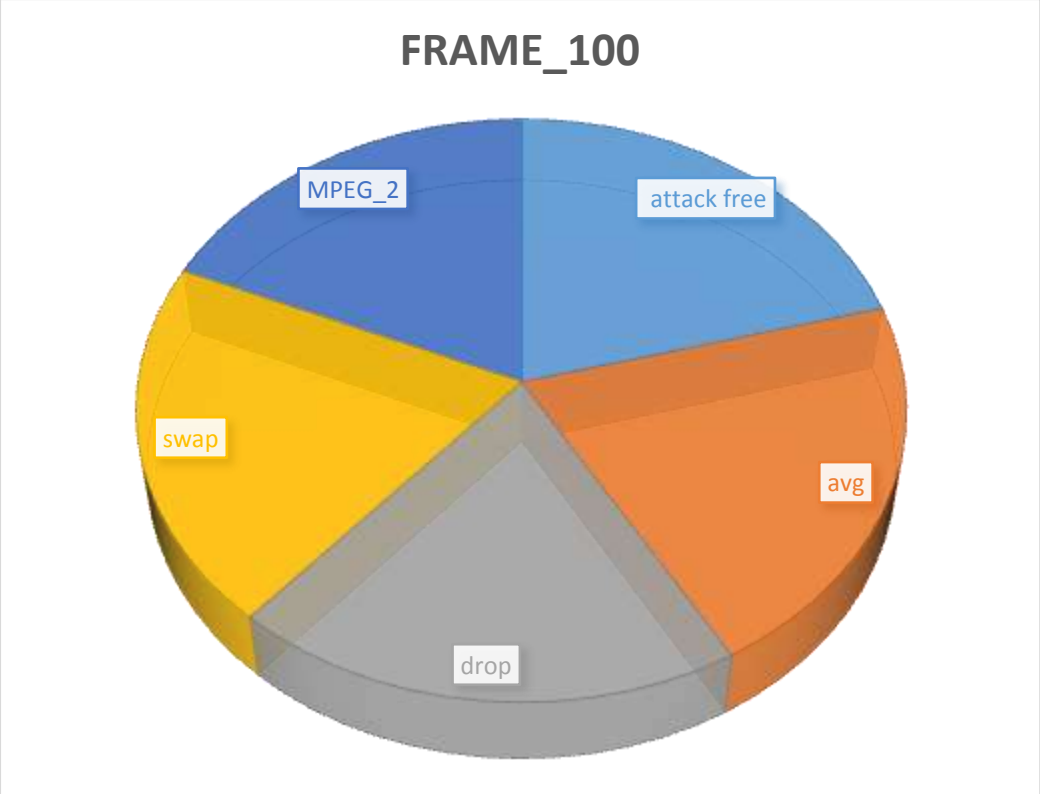

Figure 7. Graphical representation of attacks

Fig 7 & table 2 explains that different attacks on watermarked image, at this stage some of techniques has been failed because of conventional insecure methods. These are limitations in.

On another hand, frequency domain technique offers more security but at the same time it is difficult to recover the watermark at the receiver end as the complexity increases. Frequency domain techniques do not provide successful recovery of watermark. Thus, in this chapter various techniques of digital video watermarking, depending upon spatial and frequency domain techniques are discussed.

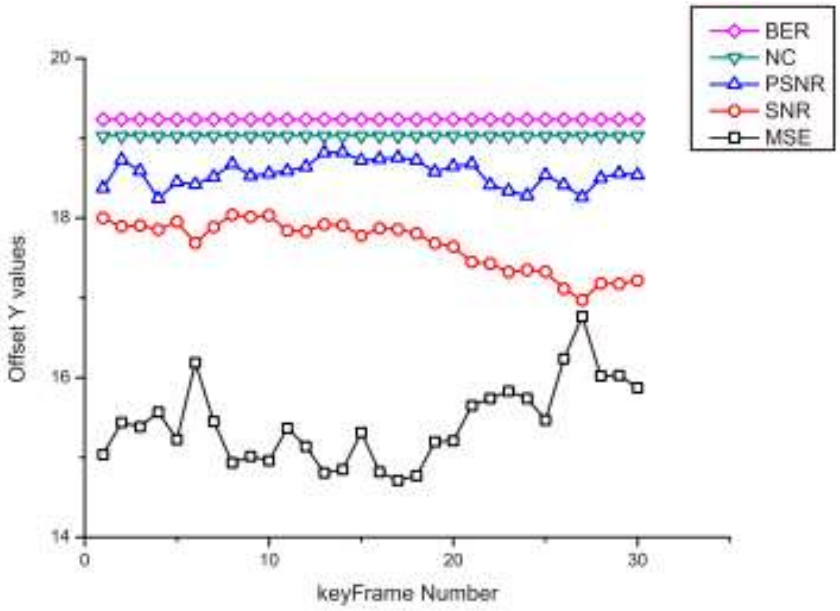

Figure 8. o-30 evaluation procedure

Fig 8 explains that different quality assessment parameters by using salience map watermarking procedure. Here bit error rate is more the NC value not near to 1, the PSNR value varies from 19.5 to 19.6, the SNR value has falling MSE is raising which are shown in figure.

CONCLUSION

Robust blind digital video watermark mechanism is implemented with logistic regression and particular video acquisition host by using no overlap collection of pictures (COP) is first designed. To ensure binary transparency digital watermark less frequency sub band wavelets are quantized at extraction process. The original real video is not required at extraction process in. This investigation suggest that robust digital watermarking with attacks like addition of noise, filtering, brightness and temporary attacks. Accuracy is 97.81%, efficiency is 95.6% and true positive rate 0.96 improved.

REFERENCES

[1] Saraju P. Mohanty, "*Digital Watermarking: A Tutorial Review*", URL: http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf http://citeseer.ist.psu.edu/mohanty99digital.htm.

[2] Bender W, Gruhl D, Morimoto N, Lu A (1996). Techniques for data hiding. *IBM Systems Journal* 35(3/4): 313-336.

[3] Arnold M, Schmucker M, Wolthusen SD (2003). Techniques and application of Digital Watermarking and Content Protection. *Eds.Northwood, Artech House.*

[4] Mohanty SP, Ramakrishnan JR, Kankanhalli MS (1999). A dual watermarking technique for images. *In Proc. ACM:* 49-51.

[5] Cox IJ, Kilian J, Leighton T, Shamoon T (1997). Secure Spread Spectrum watermarking for Multimedia. *IEEE Tras. on Image Processing* 6(12): 1673-1687.

[6] Nikoladis N, Pitas I (1998). Robust Image Watermarking in Spatial Domain. *Elsevier Signal Processing* 66(3): 385-403.

[7] Phen-Lan L (2000). Robust Transparent Image Watermarking System with Spatial Mechanisms. *Science Direct Journal of Systems and Software* 50: 107-116.

[8] Herna Hndez JR, Rodrm Hguez JM, Pe Hrez-Gonzahlez F (2000). Improving the Performance of Spatial Watermarking of Images using Channel Coding. *Elsevier Signal Processing* 80: 1261-1279.

[9] Aboutammam K, Tamtaoui A, Aboutajdine D (2009). A New Spatial Decomposition Scheme for Image Content-based Watermarking. *In IEEE/ACS International Conference on Computer Systems and Applications*: 539-542.

[10] Preda RO, Oprea C, Pirnog I, Perisoara LA (2012). Robust Digital Video Watermarking in the Spatial and Wavelet Domain. *In Proceedings of the Seventh International Conference on Digital Telecommunications (ICDT)*: 78-83.

[11] Yang G, Lucas R, Caldwell R, Yao L, Romero M, Caldwell R (2010). Novel mechanisms of endothelial dysfunction in diabetes. *Journal of Cardiovascular Disease Research* 1(2): 59-63.