Secure Irreversible Rapid Fourier Transform For Secure Communication In Video Steganography

R.Umadevi,
Part Time Research Scholar
Department of Computer Science
Periyar University, Salem,, India,
mail2deviuma@gmail.com

Dr.G.M.Nasira,
Assistant Professor.,
Department of Computer Science
Chikanna Govt. Arts College, Tirupur,
India,nasiragm99@yahoo.com

***Abstract*-Recently, several efficient data hiding algorithms has been developed successfully for video steganography. Data hiding is one promising way to accomplish better data communication by hiding information into a video medium carrier to form an unrecognizable code stream. Motion features-based approach is a popular type of steganographic algorithms related to video coding crafts. However, in most existing approaches, the choice of features on the perceived video quality mainly depends on blurring and blocking effects without considering the variance and intensity of temporal changes in irreversible video steganography. In this work, a novel method is introduced to reduce the complexity of data hiding on video steganography, Adaptive Irreversible Rapid Fourier Transform (AIRFT) technique is proposed. The polynomial hashing in AIRFT ensures lesser complexity of data hiding and achieves pseudo randomness of the output without any packet (i.e.,) information loss on the video frame. Based on the generated functions, an efficient Rapid Fourier Transform method for increasing the disguise level and generate a random like output by addressing the variance and intensity of temporal message changes is presented. Finally, the proposed video steganography method is evaluated via simulations. The simulation results evaluated with the aid of SD sequences by Video Quality Experts Group (VQEG) with parameter such as packet information loss on video frame, complexity on data hiding, Peak Signal to Noise Ratio. It shows that the method AIRFT enhance the security significantly compared with typical state-of-the-art methods.**

Keywords-Video Steganography, Features-based approach, Irreversible Rapid Fourier Transform, Rapid Fourier Transform, Temporal message

I. INTRODUCTION

With information being an influential factor in any organization, the act of sending a message to the recipient with the objective of security is one of the important issues to be addressed. So, confidentiality of the data has to be securitized in an organization with security being the main aim. Several data hiding methods have been used for embedding secret messages for several applications including copyright protection, access rights and so on. Multivariate Regression and Flexible Macroblock Ordering (MRFMO) [1] presented two data hiding technique to minimize the level of distortion using regression model. Though compression overhead was improved, robustness against channel bit errors was not resolved.

Video Quality Assessment (VQA) [2] presented a scheme to measure the assessment of video streams with the aid of salient motion region segmentation. But, variance and intensity of temporal changes remained unattended. To consider the temporal changes, Least Significant Based Approach (LSBA) [3] was designed by applying edge adaptive scheme. This improved in obtaining high quality video images enhancing the security in a significant manner. Another method based on Vector Quantization (VQ) [4] was designed to reduce the peak signal-to-noise ratio using irreversible method with the advantage of reducing the compression rate. However, the spatial and temporal aspects were not taken into consideration.

In [5], a patch based technique was introduced to reduce the peak signal to noise ratio by introducing background tessellation and temporal clustering. However, spatial nature with respect to video sequence remained unaddressed. A steganography method called, Pixel Value based Differencing (PVD) [6] was introduced to provide better security using steganalysis improving the subject and object quality.

Uploading millions ofvideos on the Internet and sharing them has become an everyday practice. Some of these videos are either illegal or being manipulated making the copyright the most stringent method. In [7], fast approximate search algorithms was designed with the motive of providing security to the videos using search algorithms improving the low positive rate and reducing the false negative rate significantly. But proper measure for fingerprint algorithms and attacks to prevent from them was not ensured. Binary image steganographic scheme was presented in [15] aims to minimize the embedding distortion on the texture. But, this scheme provides reduced image quality and less statistical protection in binary images.

Wavelet and Principal Component Analysis (WPCA) [8] was introduced to prevent attacks from Gaussian noise and median filter was introduced. Another method using greedy adaptive threshold was introduced in [9] with the objective of ensuring minimum distortion and reducing the overhead against attacks using least

significant bit. However, robustness and distortions increased with the increase in the quality of the video and data size. Video Steganography [14] approach presented to hide any type of files in any extension from carrying video file. However, this system needs additional protection while sending and receiving the secret matters.

In this paper, we propose an Adaptive Irreversible Rapid Fourier Transform (AIRFT) technique and apply it to video steganography to improve the security. The adaptive irreversible method described in this paper exploits the variance and intensity of temporal changes for video steganography. By modeling the differences between dissimilar features in cover-video frames, the method identifies distinguished frames from this technique and postulates variable size of input and provides with a fixed size as output using secure hash polynomial function. An irreversible rapid fourier transform is applied to the distinguished frames to reduce the peak signal to noise ratio. The experimental results evaluated on video files show that the results obtained are comparatively better than the state-of-the-art methods.

The rest of the paper is organized as follows: Section II provides an overview of the relevant published work on data hiding methods used for video steganography. The methodology used to determine the security, extract distinguished frames and select the best features for embedding is described in Section III. Section IV presents the experiments conducted to evaluate the applicability of the proposed techniques and AIRFT estimation results are obtained. Conclusions are provided in Section V.

II. Related Works

The process of image steganography adds messages, data, and audio files intocover images in order to obtain stego images, which is not visible to the intruder. One of the extensively used methods in image steganography is replacement of bits using Least Significant Bit (LSB) where the bits in cover image were updated with the message bits. In [10], an optimal and linear and runtime algorithms was applied to the cover video with the motive of improving the accuracy of the cover video files being sent. However, accuracy was not related to high data embedding capacity leaving room for generative model.

To improve accuracy for high data embedding in [11], a new steganography algorithm was proposed. However, the integrity of data hidden messages was not considered. Subtractive Pixel Adjacency Matrix (SPAM) [12] was introduced to improve the features being detected using support vector machines using LSB matching. The higher order utilization i.e., second order and third order LSB matching remained unsolved. Different Size Image Segmentations (DSIS) algorithm [13] was introduced to hide a huge amount of secret data presented by secret color image. But, DSIS algorithm provides low level of security.

III. Overview Of Proposed Method

A cover video is the video in which data is embedded and the video which is used for carrying secret data is termed as stego video. High-quality data hiding method should be accomplished while provided with a modifiable payload. Video Steganography consists of two schemes namely, reversible and irreversible scheme. Reversible scheme in video steganography has the ability to embed the secret data into a video and then recover the video devoid of losing any information when the secret data is extracted.

High capacity with good visual quality of stego video is not easy to achieve while embedding the secret information and so this work concentrates on developing an irreversible data hiding method. The architectural framework for generating an irreversible data hiding method called, Adaptive Irreversible Rapid Fourier Transform is shown in Figure.1.

Figure.1 shows the architecture diagram of AIRFT method. The construction of AIRFT method is divided into three parts, namely, secure hash polynomial function, irreversible rapid fourier transform and polynomial hash embedding and extraction. The first part efficiently constructs the secure hash polynomial function by obtaining the distinguished frame through hash polynomial value to reduce the complexity on data hiding. The application of polynomial hash value in AIRFT method increases the security. The second part designs an effective irreversible rapid fourier transform to reduce the peak signal to noise ratio by XORing the binary map. Finally, hash polynomial embedding and extraction algorithm is described. The elaborate description of each part is explained in the forthcoming sections.

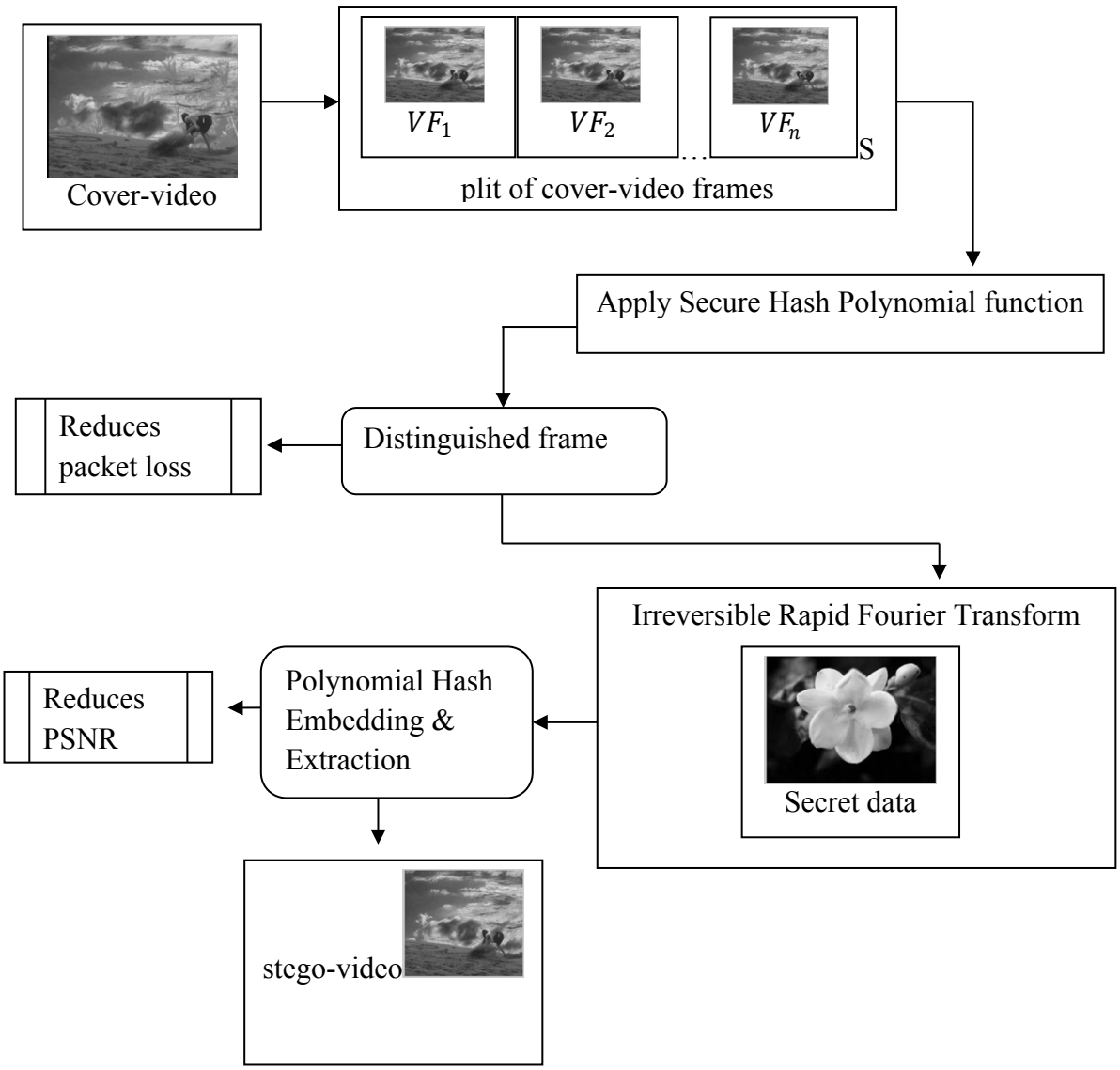

Figure 1. Architectural structure of AIRFT method

A. Construction of secure hash polynomial function (reduces complexity on data hiding and improves security)

Data hiding in video is not similar to that of image due to the inclusion of temporal information in the video. Let us consider a video file 'VF'that is split into sequence of images 'VF_1,VF_2,..,VF_n. As data hiding (i.e., temporal details) in each image of the video file involves time consuming process, the temporal details are only hid in distinguished frames. Upon successful detection of distinguished frames, the temporal details are added. Otherwise, data hiding is not performed. This reduces the complexity on data hiding. The detection of distinguished frames is detailed in the coming section.

B. Detection of distinguished frame (reduces information or packet loss)

The first step in the design of AIRFT method is the detection of distinguished frame by measuring the boundaries positions in video sequences. Due to the popularity of hash algorithms with their state changing from natural to unnatural, several hash functions were used for detection of distinguished frame. In this work, we present a Secure Hash Polynomial function with the objective of reducing the information loss.

To evaluate the Secure Hash Polynomial function, time series of dissimilarity features for each frame is obtained. Let us consider that for each frame, there includes dissimilarity features 'F_n'. Then, the dissimilarity feature for frame $F_n$is given as below

$$F_n = Dissimilar(n-1, n) \tag{1}$$

With the obtained dissimilarity feature, let the distinguished frame be '$F_n(\propto_{w,h})$', where the subscripts w and h represents the width and height. Then, the hash polynomial function takes variable size of input and provides with a fixed size as output. To make the process of steganalysis complex, in AIRFT method, dissimilarity feature is not embedded directly to each frame, but performed using hash polynomial functions. Then, the hash polynomial function is given by

$$P = Q \,\%\, R \tag{2}$$

In (2), 'P' represents the bit position, 'Q' represents the position of hidden image pixel and number of bits is specified in 'R' and the distinguished frame obtained in denoted as 'DF'. The hash polynomial function is different from conventional hash function as the hash polynomial function hide value obtained from polynomial into cover image pixels on the basis of embedding positions availability. Therefore, though the process of steganalysis is complex, but complexity involved in data hiding is reduced by applying hash polynomial function. As a result, the information loss is also reduced. Also to securitize the method, data hiding in AIRFTmethod is performed by bit distribution that sums the square value up below next value '$\beta_{i,j}$' of frame 'F_n' and performs the same up to above next value '$\gamma_{i,j}$' of frame 'F_n'. As a result, the AIRFT method ensures multi-layer security. Then, the intensity of temporal message for data hiding is evaluated as given below

$$I = (\beta_{i,j} + \gamma_{i,j})/2 \tag{3}$$

From (3), the hash polynomial value with the aid of below next value and above next value is obtained as given below

$$HP_n = Pixel(F_n) - \beta_{i,j}, \text{ if } F_n < I \tag{4}$$

$$HP_n = \gamma_{i,j} - Pixel(F_n), \text{ otherwise} \tag{5}$$

By evaluating the hash polynomial value as given above, the AIRFT method tightens the security, though the values are accidently discovered, but the actual embedded message is not revealed. So the function is said to be Secured Hash Polynomial.

C. Irreversible rapid fourier transform (minimize peak signal to noise ratio)

Based on the generated functions using Secured Hash Polynomial function, an efficient Irreversible Rapid Fourier Transform method to hide information (i.e. secret data) transform coefficients of cover images is presented for addressing the variance and intensity of temporal message changes. The irreversible rapid four transform in AIRFT method works on the principle of DCT transform. As described earlier using the secured hash polynomial, the cover-video which is split into frames are transformed to bit stream. The IRFT operates on DCT transform of '$F_n(\propto_{w,h})$' given as below

$$f(i,j) = \frac{1}{n}\sum_{w=1}^{n}\sum_{h=1}^{n} F(w,h)e^{(iw+jh)} \tag{6}$$

$$where\ F(w,h) = DCT((\propto_{w,h})) \tag{7}$$

In order to reduce the PSNR rate, the AIRFT method does not use the entire coefficient values instead it applies the following principle which generates a random like output by addressing the variance and intensity of temporal message changes. The binary map for AIRFT method is given as below

$$Map\ (w,h) = \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} \begin{matrix} if\ f(i,j) > 0 \\ otherwise \end{matrix} \tag{8}$$

From (8), the AIRFT obtains the positive values from the imaginary portion. As only the positive values are obtained, it is highly difficult for the attackers to reframe the secret data. Hence the method is said to be Irreversible Rapid Fast Transform. In other words, it is a one way function which accepts initially a user secret data. This $Map()$is XORedwhere the result is transformed into grayscale values again reshaped to obtain the ciphered image value.

The payloads (i.e., secret data) are securely embedded in AIRFT method with the aid of embedding and extraction algorithm as explained in 1.3.1. The image being embedded image is referred to as the Stego image that includes two portions namely, the Caption and the Middle. This is shown in Figure 2. The Caption part of IRFT includes the temporal content of every cover-image in the video file. On the other hand, middle part of the image includes the spatial content, if that image is identified as a distinguished frame.

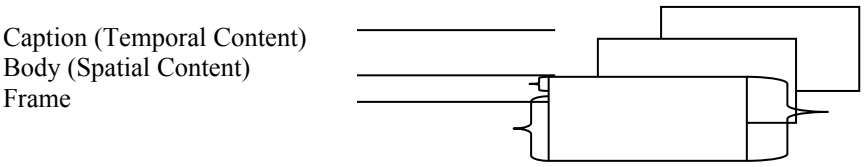

Figure 2. Representation of caption and body of stego-videos

D. Construction of Polynomial Hash Embedding and Extraction algorithm

Once the distinguished frames are obtained using Secure Hash Polynomial function and Irreversible Rapid Fourier Transform is applied to the distinguished frames, an algorithm to perform polynomial hash embedding and extraction is described. The algorithmic description of Polynomial Hash Embedding and Extraction (PHEE) is given below.

Input: cover-vide file, frames

Output: stego-video

//embedding

Begin

Step 1 For each cover-video file

Step 2 Select the .avi cover-video file and split into frames

Step 3 Select the frame according to the distinguished frame

Step 4 Convert secret message into cipher text using Secured Hash Polynomial Function

Step 5 Hidethe secret message (.text) into the cover-video frame using hash polynomial value obtained from (3)

Step 6 Transformthe original frame with stego frame

Step 7 Reconstruct the frame to form stego-video

Step 8 End for

//extraction

Step 9 Input the stego-video

Step 10 Obtain IRFT for the stego-video using (4) and (5)

Step 11 Obtain secret messages from (6) and (7) and the cover-video file

End

As given above, PHEE initially obtains the cover-video file. The cover-video file is then split into frames. The distinguished frames are obtained using Secure Hash Polynomial function. With the distinguished frames, the intensity of temporal message for data hiding is evaluated. Followed by this, the hash polynomial value is applied to it. The secret data is then hidden into the cover-video frame. The original cover-video frame is then transformed to cover-video frame. In a similar manner, to extract the original cover-video file, Inverse Rapid Fourier Transform is applied to the stego-video. Finally, the original cover-video file is obtained.

IV. EXPERIMENTAL EVALUATION OF AIRFT

The method Adaptive Irreversible Rapid Fourier Transform (AIRFT) is simulated using MATLAB. Video of different sizes and resolution are used to embed the information. Experiment is conducted mainly where the

embedded data is invisible to the observer and at the same time maximum secret image is embedded to reduce the peak signal to noise ratio. In this section, the Adaptive Irreversible Rapid Fourier Transform method is evaluated from different points of view using various frames.

The data set used in AIRFT method is based on nine SD sequences by Video Quality Experts Group (VQEG) for purposes of testing the quality of video codec. Each sequence has been encoded using five dissimilar bit-rate settings using MPEG-2 codec. Standards of the features are calculated for 110 frames of the sequences, i.e., half of the sequence frame dispersed consistently. Table I show the dataset used to test the proposed AIRFT method.

The experimental work is compared against the existing Multivariate Regression and Flexible Macroblock Ordering (MRFMO) [1] and Video Quality Assessment (VQA) [2] to identify the effectiveness of AIRFT method. The performance of the AIRFT method is measured in terms of packet information loss on video frame, complexity on data hiding, security level and Peak Signal to Noise Ratio (PSNR).

TABLE I. DATA SET USED TO TEST THE PROPOSED METHOD AIRFT

Test cover-video ID	**Cover-video**			**Secret data**	
	Name (.avi)	***Resolution***	***Size (KB)***	***Name (.jpg)***	***Size (KB)***
V1	Blossom	216 × 192	249.5	Tulip	23.4
V2	Sample	256 × 240	313.6	Lotus	25.4
V3	Car	510 × 420	223.7	Lily	43.3
V4	Sportsman	854 × 480	905.3	Jasmine	51.2
V5	Person	320 × 240	736.2	Chrysanthemum	65.3
V6	Rose	350 × 240	434.5	Sunflower	82.5
V7	Lisa	320 × 240	110.7	Daisy	56
V8	Psy2-8	320 × 240	280.5	Cowslip	18
V9	Psy3-13	320 × 240	978.3	tiger lily	45

V. DISCUSSION

The performance of Adaptive Irreversible Rapid Fourier Transform (AIRFT) method for video steganography is compared with the existing Multivariate Regression and Flexible Macroblock Ordering (MRFMO) [1] and Video Quality Assessment (VQA) [2]. The performance is evaluated according to the following metrics.

A. Impact of Packet information loss on video frame

This section discuss about the performance measure of packet information loss on video frame and comparison made with the existing methods Multivariate Regression and Flexible Macroblock Ordering (MRFMO) [1] and Video Quality Assessment (VQA) [2]. Table II shows the result of packet information loss versus the varying cover-video size. To better perceive the efficacy of the proposed AIRFT method substantial experimental results are illustrated in Figure 3 and compared against the existing MRFMO [1] and VQA [2].

Packet information loss on video frame is the ratio of difference between the cover-video (i.e., size in terms of KB) sent and the cover-video received to the cover-video sent. It is measured in terms of percentage (%). Lower the packet information loss on video frame more efficient the method is.

$$PIL = \frac{(VF_S) - (VF_R)}{VF_R} \tag{9}$$

Packet information loss (Using proposed AIRFT) = (249.5 – 195.3) / 195.3 * 100 = 27.75
Packet information loss (Using proposed MRFMO) = (249.5 – 183.5) / 183.5 * 100 = 35.96
Packet information loss (Using VQA) = (249.5 – 171.5) / 171.5 * 100 = 45.48

TABLE II. TABULATION FOR PACKET INFORMATION LOSS ON VIDEO FRAME

Size of cover-video (KB)	**Packet information loss on video frame (%)**		
	AIRFT	**MRFMO**	**VQA**
223.7	25.83	31.33	41.35
249.5	28.25	36.13	46.16
313.6	31.45	34.25	49.25
434.5	30.25	31.13	41.35

736.2	33.55	37.25	44.52
434.5	38.58	41.25	48.35

Results are presented for different number of sizes of cover-video with differing frame size for video steganography. The packet information loss on video frame for several packets with varying cover-video sizes sent at the speed of 30 ms is shown below. The results reported here confirm that with the increase in the size of cover-video being sent, the packet information loss on video frame also increases. The process is repeated for 6 cover-video frames for conducting experiments.

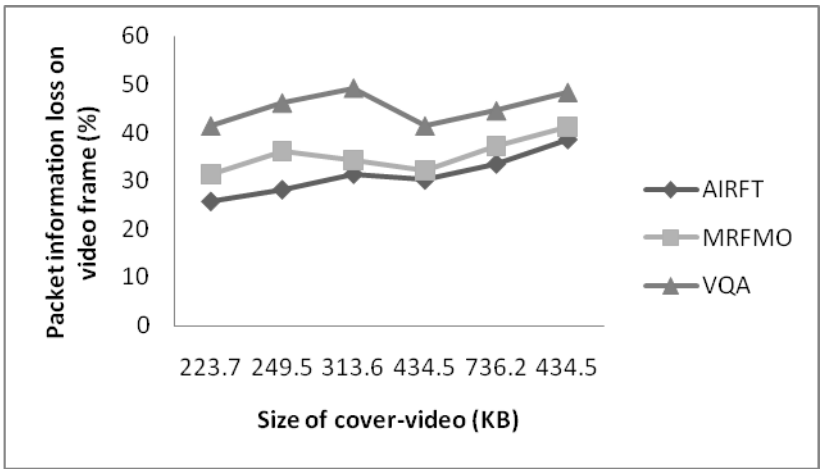

Figure 3. Measure of packet information loss

In order to investigate the packet information loss by video files to perform validations while keeping up with packet receptions, we simulated verifying both MRFMO and VQA for different implementation runs. As illustrated in Figure 3, the proposed AIRFT method performs relatively well when compared to two other methods MRFMO [1] and VQA [2]. The packet information loss on video frame is reduced in the proposed AIRFT method by efficiently detecting the distinguished frame using Secure Hash Polynomial function.

The packet information loss in AIRFT method is decreased by removing the dissimilar features by applying hash polynomial function which obtains variable size input and results in fixed size output. Therefore the packet information loss is reduced in AIRFT method by 6 – 27 % compared to MRFMO Moreover, in AIRFT method using hash polynomial function, according to the embedding positions availability, the hash polynomial function hide value obtained from polynomial resulting in minimum information loss by 13 – 47 % compared to VQA.

B. Impact of complexity on data hiding

In order to reduce the complexity on data hiding for different size cover-video files for video steganography, the time taken to hide data using distinguished frames is considered. In the experimental setup the size of cover-video ranges from 223.7 KB to 434.5 KB is provided in Table III. The complexity on data hiding using the method AIRFT provides comparable values than the state-of-the-art methods.

Complexity on data hiding is the time taken to perform data hiding process using distinguished frames. It is measured in terms of milliseconds. It is the product of distinguished frame obtained for data hiding and the time taken to hide for that distinguished frame (i.e., ms). It is given as below

$$DH_c = DH_{DF} * Time \quad (10)$$

Complexity on data hiding (Using proposed AIRFT) = (210.5 * 0.5) = 105.25
Complexity on data hiding (Using proposed MRFMO) = (215.3 * 0.5) = 107.65
Complexity on data hiding (Using VQA) = (221.2 * 0.5) = 110.6

TABLE III. TABULATION FOR COMPLEXITY ON DATA HIDING

Size of cover-video (KB)	Complexity on data hiding (ms)		
	AIRFT	MRFMO	VQA
223.7	106.45	108.25	111.35
249.5	175.35	192.35	195.15
313.6	213.45	220.38	235.15
434.5	205.81	215.15	223.15
736.2	239.35	241.35	249.16
434.5	245.15	252.31	259.35

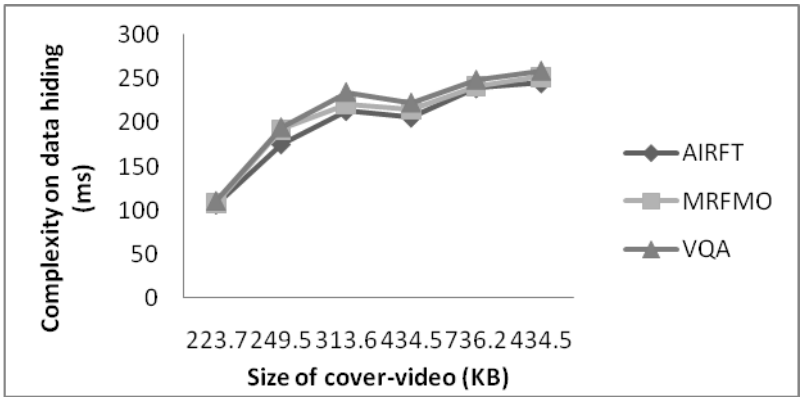

Figure 4. Measure of complexity on data hiding

The targeting results of distinguished frame to measure the complexity on data hiding using AIRFT method is compared with two state-of-the-art methods MRFMO [1] and VQA [2] in Figure 4 is presented for visual comparison based on different cover-videos of differing sizes. Our method differs from the MRFMO and VQA in that we have incorporated inclusion of temporal details that temporal information in the video. With the objective of reducing the complexity of data hiding, temporal details are only included in the distinguished frame which reduces the complexity using AIRFT method by 2 – 9 % compared to MRFMO and 64 – 84 % compared to VQA respectively.

C. Impact of peak signal to noise ratio

Peak signal to noise ratio is defined as the ratio between the maximum power of a signal and the power of unwanted noise that affects the reliability of video frames representation. PSNR is usually expressed in terms of the decibel (dB).The PSNR is measured between AIRFT method, MRFMO and VQA.

PSNR is most simply defined through the mean squared error (*MSE*).

MSE = (Original frame – noisy frame) ^{2}

$$PSNR = 10\ log_{10}\left(\frac{MAX^2}{MSE}\right)$$

$$PSNR = 20\ log_{10}\ Max - 10\ log_{10}\ MSE \quad (11)$$

Mean square error = $(10 - 3)^2 = 49$
PSNR (Using proposed AIRFT) = 20 $\log_{10}$ (255) – 10 $\log_{10}$ (49) =20 (2.40) – 10 (1.69) =33 dB

Mean square error =$(10\text{-}5)^2$ =25
PSNR (Using MRFMO) = 20 $\log_{10}$ (255) – 10 $\log_{10}$ (25) =20(2.40) – 10 (1.39) =34 dB

Mean square error = $(10 - 6)^2$=16
PSNR (Using VQA) = 20 $\log_{10}$ (255) – 10 $\log_{10}$ (16) =20 (2.40) – 10 (1.20) =36 dB

TABLE IV. TABULATION FOR PEAK SIGNAL TO NOISE RATIO

video frame size(MB)	PSNR (dB)		
	AIRFT	MRFMO	VQA
10	33.2	34.6	35.7
20	34.3	36.5	40.8
30	35.4	38.2	44.3
40	38.3	43.5	48.2
50	42.1	46.8	51.9
60	44.7	53.5	57.7

Table IV shows the PSNR for AIRFT method, MRFMO and VQA versus different sizes of cover video. The signal to noise ratio of MRFMO and VQA increases gradually though not linear for differing sizes. However, the PSNR values are decreased in AIRFT as compared to other methods.

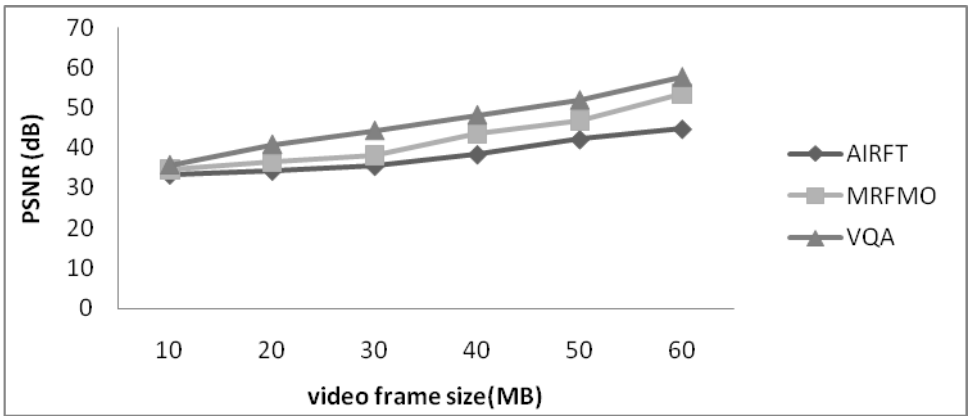

Figure 5. Measure of peak signal to noise ratio

Figure 5 illustrates the peak signal to noise ratio using AIRFT method is compared with two state-of-the-art methods MRFMO [1] and VQA [2] is presented for visual comparison based on different cover-videos of differing sizes. The Peak signal to noise ratio is reduced in AIRFT method by applying irreversible rapid Fourier transform for addressing the variance and intensity of temporal message changes. This transform also used to distinguished frames and reduces the peak signal to noise ratio. With the objective of reducing the PSNR, using AIRFT method by 4 – 19 % compared to MRFMO and 7- 29 % compared to VQA respectively.

VI. CONCLUSION

Video steganography has become an important paradigm for data hiding involving images, audio, and video as cover media. Currently, there are many video steganography methods that offer different methods for efficient data hiding with different performance attributes. With the growing number of data hiding methods, it has also becomes challenging to apply it while sending packets or information which can satisfy their QoS requirements in terms of metrics such as complexity. In this context, this work presents the technique AIRFT, to systematically measure the QoS attributes like data hiding complexity using a novel Secure Hash Polynomial Function and an efficient Rapid Fourier Transform method. An algorithm, polynomial hash embedding and extraction are also performed to reduce the noise rate based on different cover-video files with different sizes of secret data. Experiments conducted using different cover-video and secret data shows that the AIRFT outperforms in terms of data hiding complexity, packet information loss on video frame and PSNR when compared to the state-of-the-art methods. Moreover this method used for our research extension to some other QoS factor will have been applied and analyzed.

REFERENCES

[1] Tamer Shanableh, "Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering," IEEE Transactions On Information Forensics And Security, vol. 7, No. 2, April 2012.

[2] DubravkoC ulibrk, Milan Mirkovic, Vladimir Zlokolica, Maja Pokric, Vladimir Crnojevic, and Dragan Kukolj, "Salient Motion Features for Video Quality Assessment," IEEE Transactions On Image Processing, vol. 20, No. 4, April 2011.

[3] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions On Information Forensics And Security, vol. 5, No. 2, June 2010.

[4] Wei-Jen Wang, Cheng-Ta Huang and Shiuh-Jeng Wang," VQ Applications in Steganographic Data Hiding Upon Multimedia Images",IEEE Systems Journal, vol. 5, No. 4, December 2011.

[5] Andrea Colombari and Andrea Fusiello, "Patch-Based Background Initialization in Heavily Cluttered Video",IEEE Transactions On Image Processing, vol. 19, No. 4, April 2010.

[6] Weiqi Luo, Fangjun Huang, Jiwu Huang, "A more secure steganography based on adaptive pixel-value differencing scheme", Network Security and Cryptography, Springer, Jan 2010.

[7] Mani Malek Esmaeili, Mehrdad Fatourechi, and Rabab Kreidieh Ward, "A Robust and Fast Video Copy Detection System Using Content-Based Fingerprinting", IEEE Transactions On Information Forensics And Security, Vol. 6, NO. 1, March 2011.

[8] Xiaoli Li, Sridhar (Sri) Krishnan, and Ngok-Wah Ma, "A Wavelet-PCA-Based Fingerprinting Scheme for Peer-to-Peer Video File Sharing", IEEE Transactions On Information Forensics And Security, Vol. 5, NO. 3, September 2010.

[9] Hussein A. Aly, "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error", IEEE Transactions On Information Forensics And Security, vol. 6, No. 1, March 2011.

[10] Tu-Thach Quach, "Optimal Cover Estimation Methods and Steganographic Payload Location", IEEE Transactions On Information Forensics And Security, vol. 6, No. 4, December 2011.

[11] Yong Feng Huang, Shanyu Tang, and Jian Yuan, "Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec", IEEE Transactions On Information Forensics And Security, vol. 6, No. 2, June 2011.

[12] Tomá˘s Pevný, Patrick Bas, and Jessica Fridrich, "Steganalysis by Subtractive Pixel Adjacency Matrix", IEEE Transactions On Information Forensics And Security, vol. 5, No. 2, June 2010.

[13] Odai M. Al-Shatanawi1 and Nameer N. El. Emam2, "A New Image Steganography Algorithm Based On Mlsb Method With Random Pixels Selection", International Journal of Network Security & Its Applications (IJNSA) vol.7, No.2, March 2015.

[14] Snehal Satpute ,Sunayana Shahane,Shivani Singh, Prof.Manisha Sharma, "An Approach towards Video Steganography Using FZDH (Forbidden Zone Data Hiding)", International Journal of Innovations & Advancement in Computer Science (IJIACS) ISSN 2347 – 8616, vol 4, No. 1, January 2015.

[15] Bingwen Feng, Wei Lu, and Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE Transactions On Information Forensics And Security, Vol 10, No. 2, February 2015, pp. 243-255.