



VIDEO STEGANOGRAPHY TECHNIQUE FOR ROBUST MULTIMEDIA COMMUNICATIONS USING EMSBI, AIRFT AND APVQ METHOD

Dr.R.UMADEVI

SECURE COMMUNICATION

VIVEKANANDHA COLLEGE OF ARTS AND SCIENCES FOR WOMEN (AUTONOMOUS)

1. Introduction

The steganography techniques are used to hide the secret message and make it complicated for attackers to find the occurrence of the messages. Here, Video Steganography is focused where the data hiding is carried out in the video files. A video in which data is embedded is referred as a cover video and the video which is used for carrying secret data is termed as stego video. Video Steganography consists of the reversible and irreversible scheme. The reversible scheme 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. The robustness of video code streams are maintained by designing Enhanced Most Significant Bit Irreversible method. After improving the robustness value, polynomial hashing in AIRFT technique achieves higher security on video steganography. Vector quantization model improves the performance level on video code streams without compromising the video quality. Our research work on steganography focuses on images, audio, and video as cover media.

The aim of our research work is to maintain robustness on video code streams and to improve the security on video steganography and to improve the performance level on video code streams without compromising the video quality. The main objective of our research work is,

- To maintain robustness on video code streams, Enhanced Most Significant Bit Irreversible (EMSBI) method is designed.
- To reduce the prediction error rate and to improve the robustness value, the irreversible contrast mapping is used in EMSBI method.
- To improve the security on video Steganography, Adaptive Irreversible Rapid Fourier Transform (AIRFT) technique is developed.
- To improve the performance level on video code streams without compromising the video quality, Adjoin Prediction and Vector Quantization (APVQ) model is proposed and to achieve better visual quality of information with minimal runtime, Video Region Match Vector Quantization is employed in APVQ model.

2. Review of Literature

A significant improvement in computer systems has resulted in the introduction of new technologies for video steganography. In order to determine certain models and their applications has extensively developed with the aid of literature. Wei-Jen Wang., et al. (2011) developed Vector Quantization (VQ) based on data-hiding method, that has the ability of extracting the secret data from the stego-image. However, reversible method produces the code streams with low capacity secret data. Hussein A. Aly., (2011) presented Greedy Adaptive Threshold (GAT) method which performed the secret message compression on video files integrating MPEG-2 encoder/decoder. But, GAT included higher prediction error and embedded payload failed to maintain robustness on code streams.

Dubravko C. Ulbrich, et al. (2011) planned Video Quality Assessment (VQA) to measure the assessment of video streams with the aid of salient motion region segmentation. But, variance and intensity of temporal changes is remained unsolved. Tamer Shanableh, (2012) introduced Multivariate Regression and Flexible Macro block Ordering (MRFMO) to minimize the level of distortion using regression model. Though compression overhead was improved, but robustness against channel bit errors was not resolved. Babloo Saha and Shuchi Sharma, (2012) briefed data hiding using steganography techniques called as Spatial Domain based Graphical (DSG) to address the issues related to security.

Punam Bedi, et al. (2013) developed data hiding scheme based on spatial domain where Particle Swarm Optimization was applied to ensure image quality and to the distortion tolerance. Tseng-Jung Lin, et al. (2013) designed Data hiding using discrete cosine transform that preserved the visual quality at a greater level with the help of error propagation scheme. Ratnakirti Roy, et al. (2013) briefed edge adaptive image steganography method which included both advantages of matrix encoding and least significant bit matching for data embedding by applying chaotic mapping method to improve the security.

R.S. Gutte, et al. (2013) presented Extended Substitution Algorithm offers the security in internet with minimizes the error. But reliability was unaddressed in this model. Kousik Dasgupta, et al. (2013) briefed GA based Optimized video Steganographic method with the support of cost function. However, the method was not susceptible to security. Hamdy M. Kelash, et al. (2014) introduced a novel algorithm for improving the security and embedding capacity with minimize the faded pixels by using LSB substitution. Hamdy M. Kelash, et al. (2014) explained steganography based on color histogram to guarantee integrity and to improve the security for the images being extracted. Remi Cogranne, et al. (2014) designed decision theory and quantized samples with the objective of reducing the false alarm rate with quantized observation. Pye Aung and Tun Min Naing, (2014) developed an integrated Advanced Encryption Standard (AES) and Discrete Cosine Transform (DCT) to improve the security of data being sent.

Bingwen Feng, et al. (2015) explained binary image steganography scheme to preserve effective the quality of image and embedding capacity through local texture patterns. However, false alarm rate increased with the increase in the number of images being submitted. Based on the above mentioned methods and techniques, the following proposed works aim to provide an appropriate solution to solve the existing issues. R.Umadevi (2015) developed EMSBI, AIRFT and APVQ methods for better embedding efficiency, security and video quality respectively.

All the above literature reveals that the existing methods and technique has its own limitations with its own merits and demerits. To overcome these limitations, we have proposed an appropriate methodology to meet the existing issues and pitfalls.

3. Motivation and Need for Research

- Steganography techniques has revealed extensive success in image processing since it cover the secret message and make it complicated for attackers to find the occurrence of messages. Video steganography is the process of hiding the secret data inside the video.
- Despite its popularity, the lack of embedded payload using reversible method remains a significant challenge to maintain the robustness on code streams in low prediction-error environments. Unfortunately, these reversible methods produce the code streams with low capacity secret data resulting in higher prediction error. For these parameter improvements, we provoked to design proposed method.
- Besides, several efficient data hiding algorithms have been developed for video steganography, motion features-based approach is a popular 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 order to we initiated our research to produce better results in the video quality.
- In addition, the swift progress of data transfer through internet has made data to reach the destination at a faster manner. At the same time, the data being transferred through internet can be reorganized and misused through hacking.
- Most of the research work has been carried out for image hiding scheme using Particle Swarm Optimization (PSO) method and Structural Similarity (SSIM) indexes, but compromising image quality when applied to video frame and reversible method not effective in producing high performance code streams. In order to overcome such limitations in video steganography, the proposed methodology is designed.

4. Frame work of proposed methodology

The proposed research work focuses on maintaining robustness on video code streams and to improve the security on video steganography and to improve the performance level on video code streams without compromising the video quality. The proposed research work is carried out in three phases as shown in Figure 1.

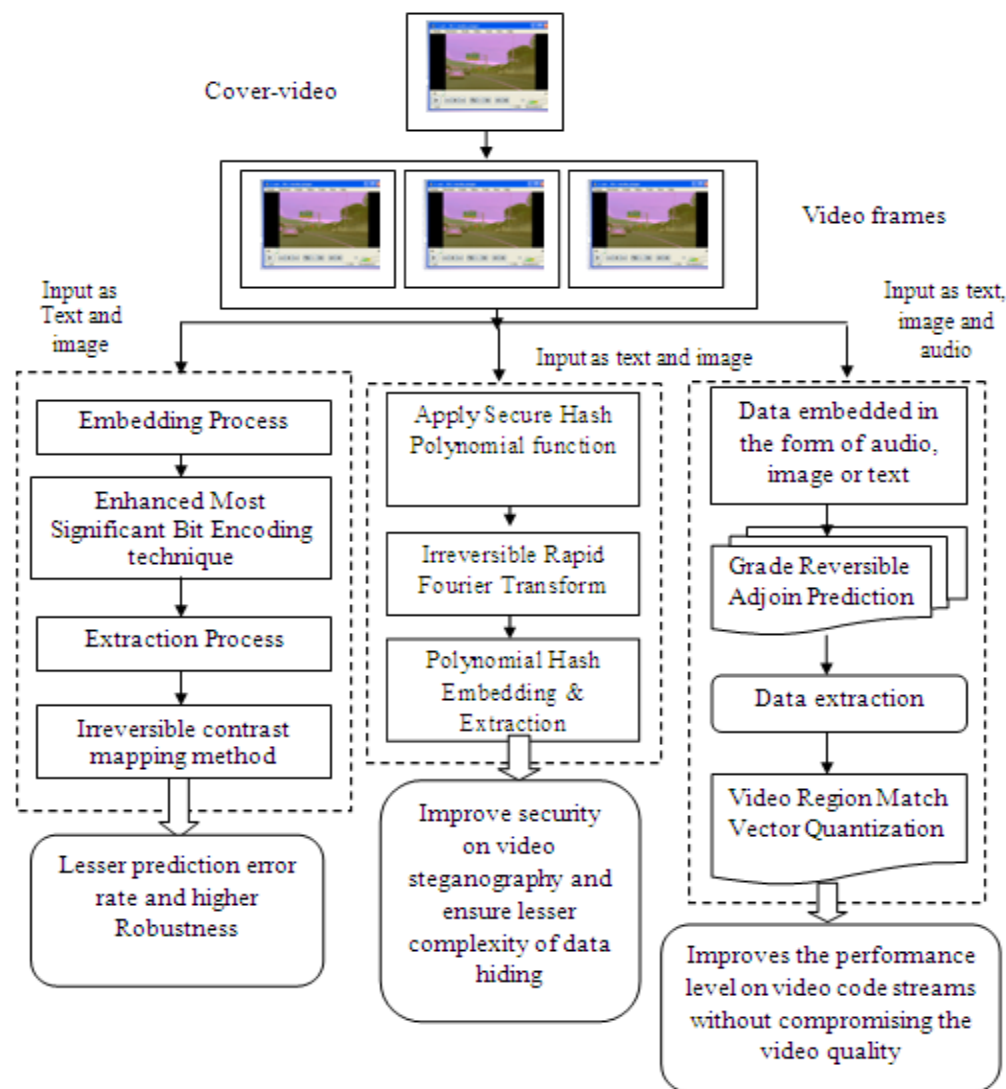


Figure 1 Frame work of proposed Methodology

Figure 1 illustrates the flow process of three proposed methodologies for improving the security on video steganography and to improve the performance level on video code streams without compromising the video quality. The detailed explanation about the proposed methods is detailed described in following subsections.

5.1. Enhanced Most Significant Bit Irreversible Method on Video Steganography

The design of enhanced most significant bit irreversible method is presented on video steganography with the help of embedding and extraction processes. The main objective of proposed method on video steganography is to produce the code streams with high capacity secret data. Initially, the embedding process is performed in which the secret message bits are embedded in the form of binary value on the cover video frame. The binary values are employed to cover the secret information and are placed inside the video file. After encoding the secret information, the information is extracted on the receiver side to discover the secret information. With the application of irreversible contrast mapping, the effectiveness of proposed EMSBI method is improved by means of minimizing the prediction error rate and improving the robustness value.

5.1.1. Embedding Process for data hiding

Our EMSBI method perform embedding process which efficiently embed the secret information with the video file and produce the Stego video files as the output during this process. Initially, a cover video file is chosen as input where the secret information is to be embedded and then embedding process is performed. In EMSBI method, the embedding process

performs binary value conversion on the secret information. It effectively performs the embedding process without any error difference between the original coefficients value and the embedded coefficient values. The altered value checks the next right bit to be modified to perform the embedding process. With this, the binary value conversion on the embedded side, improves the information secrecy.

5.1.2. Steps carried out for encoding process

Next, EMSBI method performs encoding process with the application of enhanced most significant bit. The secret data is placed randomly on the video file and the encoding operation is carried out with where the secret information has to be steganographed. The video frames identify the authenticated person easily by using stego key and transmits the secret information. The most significant bit encoding technique is modified slightly with segment filter encoding scheme that segments the video file and hide the data. The segment filter encoding divides the whole video file into frames for easy operation during embedding process. They embed the secret data using the pixel coefficient value on the video file and perform the segment filter encoding. The segment filter encoding process employs the spatial prediction and motion estimation to minimize the prediction error rate to be encoded. At the extraction process, the encoder derives the prediction information by subtracting the predicted frame from the original video frame using EMSBI method.

5.1.3. Process of Extraction

After obtaining the Stego video files at the transmitter side, the receiver precisely reverses the process using the enhanced MSB irreversible method. Using the Stego video file, the EMSBI method extracts the secret data. Finally using the EMSBI method, the original image is obtained using the irreversible contrast mapping method. Once the secret information is extracted, the enhanced MSB prediction error and PSNR ratio on extraction of secret data using the EMSBI method is evaluated. The secret information is embedded on different video frames.

5.1.4. Irreversible contrast mapping method for extraction

Irreversible contrast mapping on the extraction side, offer high capability data extraction on the code streams. The extraction work is carried out effectively using the exact Stego key values. Irreversible contrast mapping substitutes the Most Significant Bit of 'p' with 'q' and Most Significant Bit of 'q' with 'p'. Enhanced MSB of 'p' is set to 'x-axis dimensional space' to indicate their transformed pair, while zero otherwise. The pixel coefficients values of the frame are transformed to obtain the hidden secret information. However, the exact coefficients provided at different levels therefore desirable to obtain the information with higher robustness.

5.2. Adaptive Irreversible Rapid Fourier Transform Technique

As the discussion of section 1, initially, secure hash polynomial function is presented for provide the multi-layer security to the modular additions and density function. Polynomial hashing provides minimum complexity of data hiding and attains the information without any loss on the video frames. Next, an efficient Rapid Fourier Transform method is introduced based on the generated function for increasing the disguise level. Finally, Polynomial hash embedding and extraction algorithm performs noise rate based on different cover-video files with different sizes of secret data.

5.2.1. Secure Hash Polynomial Function

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 ' $VF_1, VF_2, \dots, VF_n$ '. 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.

The AIRFT method performs the detection of distinguished frame by measuring the boundaries positions in video sequences. In AIRFT method, Secure Hash Polynomial function is presented with the objective of reducing the information loss. Time series of dissimilarity features for each frame is obtained for the evaluation of secure hash polynomial function.

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, 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 and ensures multi-layer security. Then, the intensity of temporal message for data hiding is evaluated. By evaluating the hash polynomial value, the AIRFT method tightens the security, though the values are accidentally discovered, but the actual embedded message is not revealed. So the function is said to be Secured Hash Polynomial.

5.2.2. Irreversible Rapid Fourier Transform

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. It addresses the variance and intensity of temporal message changes. The irreversible rapid four transform in AIRFT method works on the principle of DCT transform. By using the secured hash polynomial, the cover-video which is split into frames are transformed to bit stream.

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 AIRFT method 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.

The payloads (i.e., secret data) are securely embedded in AIRFT method with the aid of embedding and extraction algorithm as explained in 5.2.3. The image being embedded image is referred to as the Stego image that includes two portions namely, the Caption and the Middle. 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.

5.2.3. Construction of Polynomial Hash Embedding and Extraction Algorithm

Once the distinguished frames are obtained using Secure Hash Polynomial function, Irreversible Rapid Fourier Transform is applied to the distinguished frames. Our algorithm Polynomial Hash Embedding and Extraction Algorithm (PHEE) initially obtain 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. The figure 2 shows clearly stated the original, cover and stego image.



Figure 2 (a) Original image

2(b) Cover image

2(c) Stego image

5.3. Design of Video Steganography based on Adjoin Prediction and Vector Quantization

Our research contribution Adjoin Prediction and Vector Quantization (APVQ) method is proposed to improve the performance level on video code streams without compromising the video quality. The APVQ method used to two techniques for improving the performance level on video code streams such as Grade Reversible Adjoin Prediction (GRAP) and Video Region Match Vector Quantization which are detailed described in forthcoming subsections.

5.3.1. Design of Grade Reversible Adjoin Prediction mechanism

In this section a reversible encoding mechanism called, Grade Reversible Adjoin Prediction (GRAP) is presented to enhance the performance level on video code streams. To embed secret data (i.e. image, audio or text) into the cover video frame GRAP mechanism decides the capacity of the secret data per pixel in a video frame.

In APVQ method, embedding process starts with the input as cover video file. The cover video file is split into several video frames. In each frame, horizontal differences and vertical differences view of cover video file is obtained. In the encoding side, secret data is embedded accordingly with GRAP mechanism.

For each cover video frame, before performing the data hiding process, Grade Reversible Adjoin Prediction efficiently predicts the adjoin neighboring pixels through which the data hiding process can be performed. In order to predict

the adjoining neighboring pixels, grade reversible method is applied where the horizontal view of cover video frame and vertical view of cover video frame is obtained.

Based on these two values, the new ' i' ' value and pixel region ' PR_i ' values are obtained that forms the adjoining neighboring pixels where the actual data hiding (i.e. audio, image or text) is embedded. It also embeds an index value in each video frame to ensure that the secret data recovered back with higher quality rate on decoding side. The index value points to the adjoining secret key of a state secret frame to easily achieve the performance rate.

5.3.2. Design of Video Region Match Vector Quantization

Once the effective embedding is performed using Grade Reversible Adjoin Prediction where the adjoining secret key of a state secret frame easily achieve the performance rate, the corresponding extraction process is performed. In the proposed Adjoin Prediction and Vector Quantization (APVQ) method, in the decoding side, Video Region Match Vector Quantization is used.

During extraction process, stego video is given as input. The Video Region Match Vector Quantization decodes the adjoining frames based on the index values. The embedded index value is decoded using the adjoining secret key of a state secret frame in the video frame to obtain the secret information. The reversible method of Video Region Match Vector Quantization evolves with better visual quality of information with minimal runtime.

```
//Extraction Process using Video Region Match Vector Quantization
Input: stego video  $CVF'_i$ 
Output: secret data ' $SD$ '
Step 1: Begin
Step 2:   Split the stego video  $CVF'_i$  into  $4 \times 4$  pixels
Step 3:   For each stego video  $CVF'_i$ 
Step 4:     Repeat
Step 5:       Using Grade Reversible Adjoin Prediction predict  $i$  and  $i'$  pixel value
Step 6:       Retrieve the least significant bits from the successive pixel value
Step 7:       Obtain the index value
Step 8:       Based on the  $i'$  pixel value and corresponding  $PR_i$  value retrieve the secret bits
Step 9:       Extract the secret data  $SD$ 
Step 10:    Until (all stego video is processed)
Step 11:    End for
Step 12: End
```

Figure 3 Extraction using Video Region Match Vector Quantization

The Video Region Match Vector Quantization uses an adjoining prediction concept in order to effectively quantize a stego video to non-overlapping 4×4 pixels. As shown in the figure 3 that describes the extraction process to obtain the secret data using adjoining prediction for each stego video. The Video Region Match Vector Quantization uses least significant bit position to obtain the index value and therefore extracts the secret data.

6. Simulations and Performance Metric Analysis

The proposed three methods such as EMSBI method, AIRFT method, APVQ method are implemented using MATLAB. The performance of proposed methods are evaluated with the metrics such as embedding efficiency, security (robustness), video quality level on reversible method.

6.1. Impact of Embedding Efficiency

The embedding efficiency using EMSBI method offer comparable efficiency measures than the state-of-the-art methods. The rate of embedding or the embedding efficiency using EMSBI method is defines the ratio for different secret data with set of pixels. When higher the embedding efficiency, more efficient the method is said to be. The performance of the EMSBI method is compared against with the existing two methods namely Vector Quantization (VQ) based data hiding methods by Wei-Jen Wang., et al. (2011) and Greedy Adaptive Threshold (GAT) method by Hussein A. Aly., (2011).

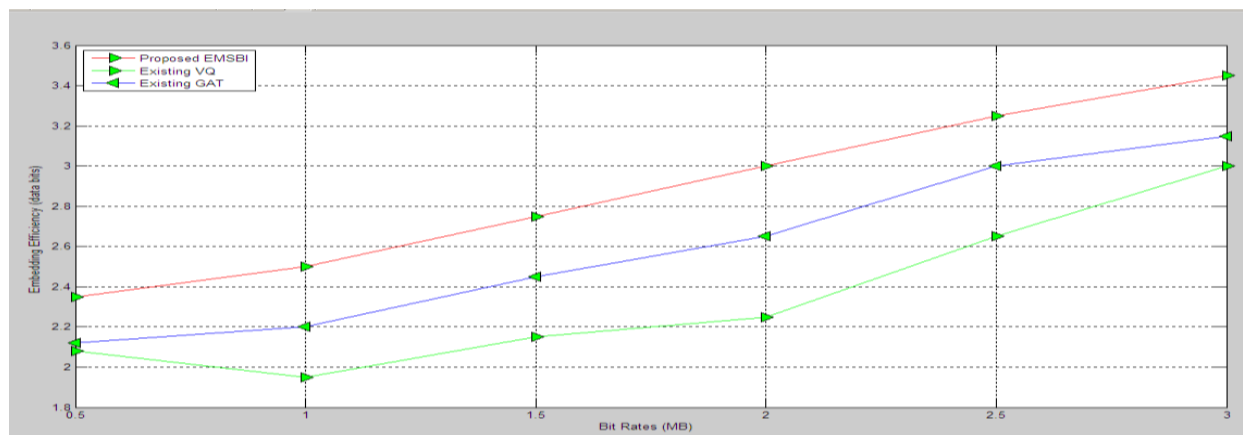


Figure 4 Measure of embedding efficiency

The targeting results of embedding efficiency rate using EMSBI method is shown in Figure 4. As shown in figure, EMSBI method provides better performance as compared to other existing methods namely, VQ and GAT respectively. This is because of the application of Enhanced Most Significant Bit encoding technique in EMSBI method. With the support of Enhanced Most Significant Bit encoding technique, EMSBI method easily improve the embedding efficiency data using the pixel coefficient value on the video file and performs the segment filter encoding which in turn improves the embedding efficiency rate by 9% as compared to VQ. For the most different sizes of bit rates, the EMSBI method achieves comparable performance to Vector Quantization and Greedy Adaptive Threshold. Therefore, the embedding efficiency is improved by 16 % when compared with the GAT.

6.2. Impact of Security (Robustness)

Security in Adaptive Irreversible Rapid Fourier Transform (AIRFT) measures the amount of noise during retrieval of secret data. The security is evaluated based on the ratio of difference between hidden secret data sent (i.e., in terms of size KB) and hidden message received. Higher the difference more securitized the method is said to be. It is measured in terms of percentage (%). The performance of AIRFT method is compared against with the existing methods namely Multivariate Regression and Flexible Macroblock Ordering (MRFMO) and Video Quality Assessment (VQA).

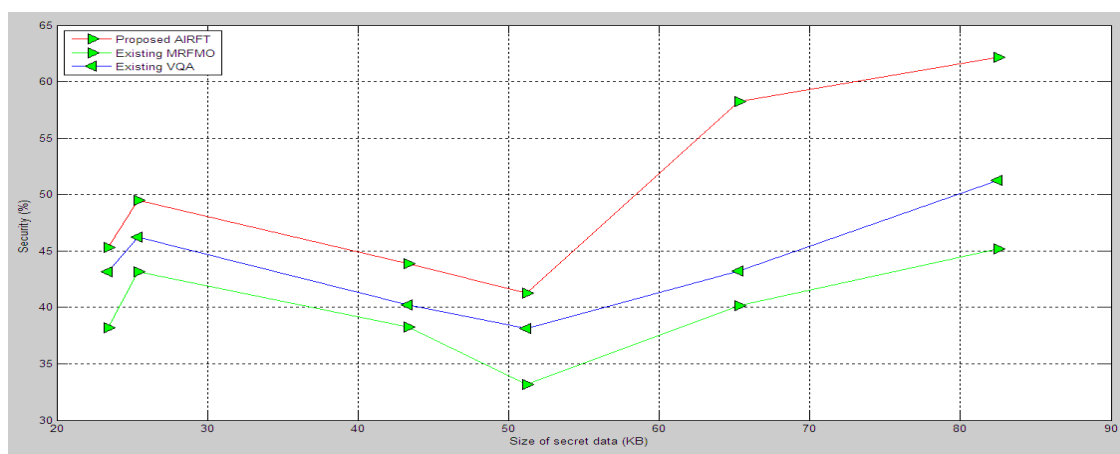


Figure 5 Measure of Security

The security of three different methods such as AIRFT method, MRFMO, VQA versus different number of size is presented in Figure 5. Besides, AIRFT method provides better performance as compared to other existing methods namely, MRFMO by Tamer Shanableh, (2012) and VQA by Dubravko Culibrk, et al. (2011). This is because with the application of bit distribution that sums the square value up below next value of frame and performs the same up to above next value of frame. With this, the security is improved in AIRFT method ensures multi-layer security. Therefore, AIRFT method improves the security by 10% as compared MRFMO and 17% as compared to the VQA respectively.

6.3. Impact of Video Quality Level on Reversible Method

The video quality level on reversible method using APVQ method is elaborated in below Figure 5. We consider the method with six different cover video for experimental purpose using MATLAB. The performance of APVQ method is compared against with the existing two methods namely data hiding in mpeg video files using PSO based Image Hiding (PSO-IH) by Punam Bedi, et al. (2013) and DCT based Data Hiding (DCT-DH) by Tseng-Jung Lin, et al. (2013).

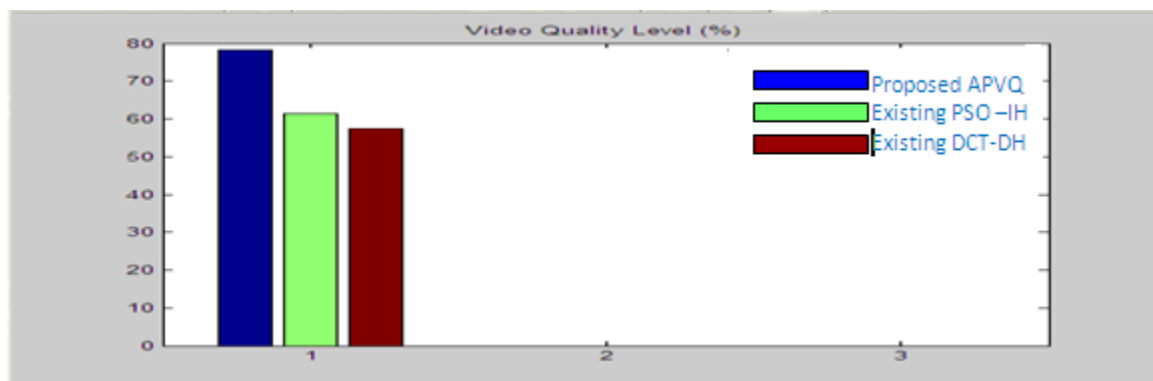


Figure 6 Measure of video quality level

Convergence characteristics of video quality level on reversible method for six cover video files with different secret data (i.e. image, audio and text) are shown in Figure 6. The targeting results of video quality level using APVQ method is compared with two state-of-the-art methods and visual comparison based on the initialization of images being considered. The method APVQ differs from the PSO-IH and DCT-DH that we have incorporated different types of secret data that efficiently improves the video quality level on reversible method. This improves the video quality level by 22% as compared to PSO-IH. With the application of Video Region Match Vector Quantization, the video quality level is improved. Further, with the aid of adjoining frames with index values, both the smaller and larger components are fine grained to fit the cover video file with higher video quality level by 27% as compared to DCT-DH respectively.

7. Conclusion and scope of the future work

Our proposed contribution Enhanced Most Significant Bit Irreversible (EMSBI) method is designed to address the problem of increasing the efficiency of embedded payload in video steganography and to maintain robustness on video code streams and to minimize the peak signal-to-noise ratio. Besides, Adaptive Irreversible Rapid Fourier Transform (AIRFT) technique is proposed to improve the security on video steganography based on variance and intensity of temporal changes. In addition, our third proposed contribution a reversible encoding method called Adjoin Prediction and Vector Quantization (APVQ) is developed to produce high performance code streams and to improve the performance level on video code streams without compromising the video quality. The future direction of our proposed work provides an embedded secret data with reduced hiding complexity on video files in video steganography. Future work performs hiding secret data information with providing a more security based on different cover-video files.

REFERENCES

- [1] 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.
- [2] 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.
- [3] Dubravko Culibrk, 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.
- [4] 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.
- [5] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No. 1, January 2012.
- [6] Punam Bedi, Roli Bansal and Priti Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance", Elsevier, Volume 39, Issue 2, February 2013, Pages 640 – 654.

- [7] Tseng-Jung Lin, Kuo-Liang Chung, Po-Chun Chang, Yong-Huai Huang, Hong-Yuan Mark Liao and Chiung-Yao Fang, "An improved DCT-based perturbation scheme for high capacity data hiding in H.264/AVC intra frames", Elsevier, Volume 86, Issue 3, March 2013, Pages 604 – 614.
- [8] Ratnakirti Roy, Anirban Sarkar, Suvamoy Chatterjee, "Chaos based Edge Adaptive Image Steganography", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.
- [9] Kousik Dasgupta, Jyotsna Kumar Mondal, Paramartha Dutta, "Optimized Video Steganography using Genetic Algorithm (GA)", International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA) 2013.
- [10] R.S. Gutte, Y.D. Chincholkar and P.U. L., "Steganography For Two And Three LSBs Using Extended Substitution Algorithm", ICTACT Journal On Communication Technology, March 2013, Vol: 04, Issue: 01.
- [11] R.Umadevi, Dr. G.M.Nasira, "Video Steganography Secure Communication System Using Enhanced Most Significant Bit Irreversible Method, International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 9, Number 23 (2014) pp. 19453-19468, © Research India Publications.
- [12] R.Umadevi, Dr. G.M.Nasira, "Achieving Secret Communication on Video files Using Steganography, International Conference on Computing and Intelligence Systems Volume: 04, Special Issue: March 2015, Pages: 1290 – 1294 ISSN: 2278-2397, International Journal of Computing Algorithm (IJCOA) 1292.
- [13] R.Umadevi, Dr. G.M.Nasira, "Secure Irreversible Rapid Fourier Transform for Secure Communication in Video Steganography", International Journal of Computational Intelligence and Informatics, Vol. 5: No. 1, June 2015 ISSN: 2349 – 6363
- [14] R.Umadevi, Dr. G.M.Nasira "Video Steganography Based on Hash Polynomial Function for Secure Communication", Indian Journal of Science and Technology, Vol 8(23), DOI:10.17485/ijst/2015/v8i34/IPL0871, September 2015, ISSN (Print) : 0974-6846, ISSN (Online) : 0974-5645.
- [15] R.Umadevi, "Joint Approach for Secure Communication using Video Steganography", IEEE 2016. Electronic ISBN: 978-9-3805-4421-2.