Analysis of Video Steganography in Military Applications on Cloud

Umadevi Ramamoorthy
Vivekanandha College for Women, Namakkal District, India
mail2umaphd@gmail.com

Aruna Loganathan
Vivekanandha College for Women, Namakkal District, India
arunaloga@gmail.com

Abstract: *The analysis of secure video file transfer with military application for video steganography on cloud computing is essential role. Video steganography is the process of hiding the secret data which is presented in the video and it is based on the reversible and irreversible schemes. The reversible scheme has the capability to insert the secret data into a video and then recover the video without any failure of information when the secret data is extracted. Irreversible methods on video steganography often deal with sensitive information, making embedded payload an important concern in the design of these data hiding systems. In video steganography, irreversible contrast mapping is considered for extracting the secret data during the process of hiding the data. During this extraction process, high quality data hiding is carried in video steganography. The analysis consequences of the proposed method Video Steganography Cloud Security (VSCS) shows that the structure for secure communication and augments the confidentiality and security in cloud. This result of the proposed method shows the better security level.*

Keywords: *Video steganography, secure communication, information security, secret data, video code streams, data hiding.*

Received April 7, 2021; accepted December 2, 2021
https://doi.org/10.34028/iajit/19/6/7

1. Introduction

Steganography techniques has exposed extensive achievement in image processing that covers the secret message and makes it difficult for attackers to find the occurrence of messages [12]. The progress of data transmission with secret data through internet has made data to reach the destination at a faster manner [9]. Data hiding process is the significant communication for data by hiding information into a video carrier to form an enhanced code stream [1, 16]. With the data communication, the hiding data provides more security for embedding the secret messages with several applications [3]. A new video steganography scheme in the wavelet domain is presented [14]. Here, is considered the military applications for transferring the secret data between different soldiers. Figure 1 illustrates the data communication between the soldiers, based on the video steganography for transferring the secret data.

The distribution service provides the defense video system for communicating the official videos to their respective organization and to collect the secret data [2, 8]. Initially, military units are distributed and transferred to other military units by generating the data files on each site for communication. Each military unit consists of respective transmitter for transferring the data files by collecting all information in a secured manner. The entire soldiers in the military are controlled by a commander with the help of the obtained secured information. A commander-in-chief provides secured communication between the soldiers and helps to easily identify the attacker offered inside the battle field. The noise variance as function of pixel expectation presented [15].

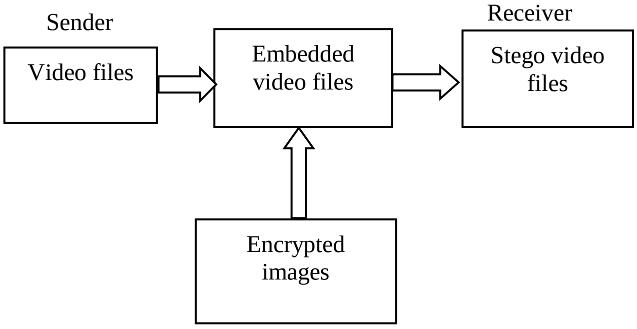

Figure 1. Data communication using video steganography in military applications.

Based on this approach, an efficient Enhanced Most Significant Bit Irreversible (EMSBI) method is to maintain robustness in data communication between the soldiers on video code streams. Increase the efficiency of the embedded payload in video steganography presented [5, 10]. EMSBI structures are highly efficient in the embedded payload of entire military networks using a high capacity secret data hiding method.

Figure 2. Video frame extraction using emsbi method.

The above Figure 2 explains about Enhanced Most Significant Bit Irreversible process for extracting secret information hided in a video files. The initial process of embedding is carried out in EMSBI method using the binary values presented in military data communication. Next, the processing of information is performed by applying Enhanced Most Significant Bit encoding technique to achieve the objective of highly efficient embedded payload. At this juncture, the binary value of the secret message is replaced with each most significant bits of the video to avoid the attackers in battle flied [7]. Finally, Irreversible contrast mapping is then carried out in military applications during the extraction process on video Steganography. During the extraction process, the high quality rate of data hiding is carried out in the video Steganography using the enhanced MSB to secure the military data. The experiment is conducted on several state-of-the-art methods to express the effectiveness of the EMSBI method.

Video steganography is an important model in military services for data hiding involving images, audio and video as cover media to send secret information [18]. There are a large number video steganography methods are presented for efficient data hiding with different performance attributes [6, 13]. Therefore, Adaptive Irreversible Rapid Fourier Transform (AIRFT) technique is used in military communication for improving the security on video steganography, based on the variance and intensity of temporal changes.

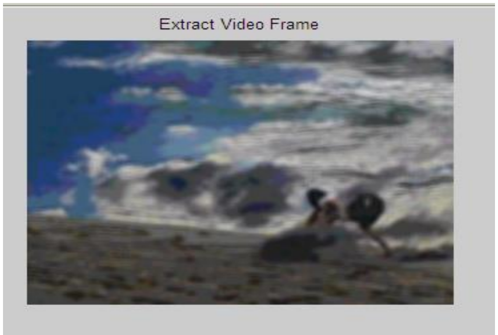

Figure 3. Video frame extraction using airft technique.

The above Figure 3 explains about Adaptive Irreversible Rapid Fourier Transform techniques for extracting information in cover-video files. The dissimilar features in cover video frames send by soldiers are identified by the distinguished video frame using secure hash polynomial function that provides more security and reduces data hiding complexity [17]. An efficient irreversible rapid Fourier transform method is applied to reduce the peak signal to noise ratio on distinguished frames send by soldiers Polynomial hash embedding and extraction algorithm are used for reducing the noise rate on cover-video files.

Finally, a reversible encoding method called Adjoin Prediction and Vector Quantization (APVQ) method is presented between soldiers without compromising the video quality to improve the performance level on video streams. To embed secret information send by military personnel into the cover video frame, Grade Reversible Adjoin Prediction mechanism is implemented which decides the capacity of the secret data per pixel in a video frame.

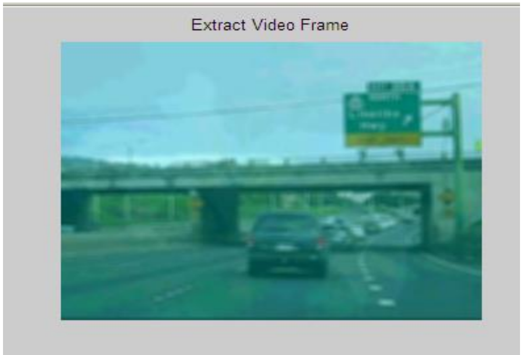

Figure 4. Extract video frame using APVQ method.

The above Figure 4 explains about Adjoin Prediction and Vector Quantization process for extracting secret information hided in a video files [4]. In the encoding side, an index value of secret data in each video frame is embedded to ensure that the secret data is recovered back by the receiver’s side in military with higher quality rate on the decoding side. The index value points to the adjoining secret key of state secret frame to easily achieve the performance level on video code streams.

In the decoding side, video region match vector quantization decodes the adjoining frames with index value points to extract the secret information [19]. The reversible method potentially attains better visual quality of information with minimal runtime [11]. Finally, the video quality and embedding capacity is adjusted and optimized according to the property of a frame in Grade Reversible Adjoin Prediction mechanism.

2. Proposed Method

In this proposed method, Most Significant Bit encoding process is conceded out for improving code stream capacity on secret data. Along with encoding operation Irreversible method is processed on video steganography for providing more security for hidden information in the system.

2.1. Encryption Method

The Stego key is used in the proposed method to secure the message file on both the embedding and extraction process. The most significant bit encoding technique is modified slightly with segment filter encoding scheme. The segment filter encoding scheme segment the video file and hide the data. The second micro-service uses Advanced Encryption Standard (AES) encryption algorithm to encrypt documents having sensitive data, which have to be transferred within the private cloud. The segment filter encoding in proposed method divides the whole video file into frames for easy operation during embedding process.

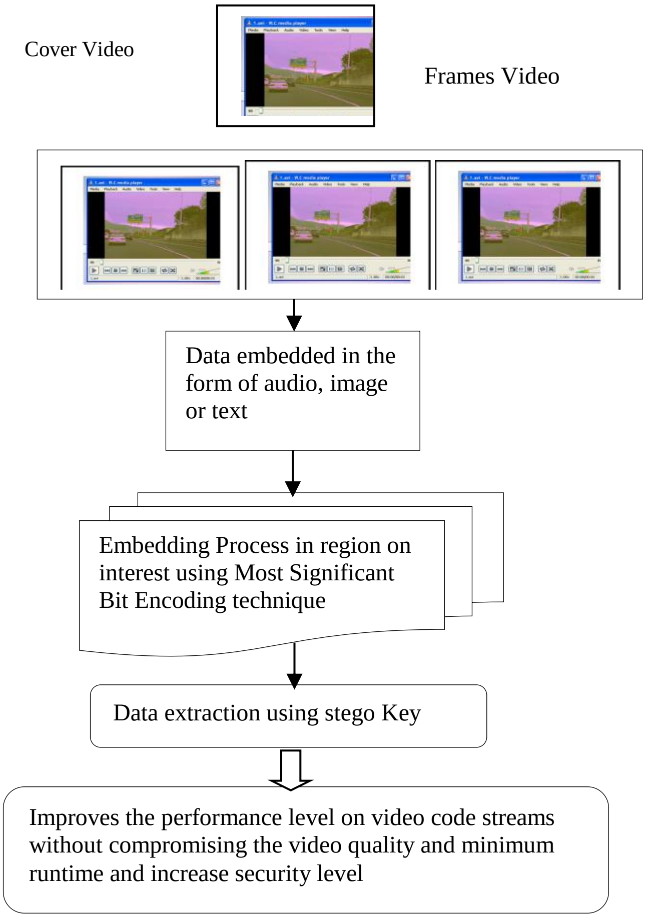
Cover Video
Frames Video
Data embedded in the form of audio, image or text
Embedding Process in region on interest using Most Significant Bit Encoding technique
Data extraction using stego Key
Improves the performance level on video code streams without compromising the video quality and minimum runtime and increase security level

Figure 5. Flowchart for proposed method.

2.2. Selection Bit Method

The enhanced most significant bit embed the secret data using the pixel coefficient value on the video file according to region on interest and performs the segment filter encoding. The Figure 5 explains 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 while sharing data in cloud. In order to analyses the performance of video file transfer, the proposed method is implemented using MATLAB. The information presented in video files is embedded with different sizes and different resolutions. Experimental evaluation is conducted for observing the embedded data of video frames which are invisible and reduce the peak signal to noise ratio with embedding the images.

In the Figure 6, our proposed work mainly deals with securing military image and textual data where cryptography, data hiding, is functional on a multimedia stuffing. A novel video steganography cloud security has been proposed for secure data transfer in cloud.

In encoding side, the military secret data has been given as input and embedded in each frame based on Region on Interest pixel. This ensures the secret on the decoding side while extract the secret data by receiver.

With the help of the compressed video files, secret images are embedded in the highest manner without any occurrence of channel bit error. The data set used in the EMSBI, AIRFT, APVQ and proposed Video Steganography Cloud Security (VSCS) methods is based 168VJ Clips video dataset and visual geometry group data for purposes of testing the quality of video codec.

Figure 6. Extract video frame using VSCS method.

3. Performance Analysis of the Parameters Based EMSBI Method, AIRFT Technique, APVQ Method and Proposed VSCS Method

The performance of the EMSBI method, AIRFT technique and APVQ method is estimated and compared with VSCS Method. The results are analyzed, based on the parameter in terms of peak signal -to- noise ratio, Robustness in Terms of Security, Execution Time. Detailed result analyses of these metrics are elaborated in further sections. The results are compared and analyzed with the help of table and graph given below.

3.1. Peak Signal to Noise Ratio Based on Video Frame Size

The average Peak Signal To Noise Ratio (PSNR) 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 frequently expressed in terms of the decibel (dB). PSNR is the most simply defined through the Mean Squared

Error (MSE).

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right) \quad (1)$$

Where, MSE=(Original frame-noisy frame)^2

$$\mathrm{PSNR} = 20\log_{10}\mathrm{Max} - 10\log_{10}\mathrm{MSE} \quad (2)$$

Table 1. Comparison of PSNR for EMSBI, AIRFT, APVQ method and VSCS method.

Video frame size (MB)	EMSBI	AIRFT	APVQ	Proposed VSCS
10	33.34	29.14	24.42	20.13
20	35.7	31.28	25.36	20.56
30	37.98	33.9	27.68	23.12
40	39.67	35.41	29.89	21.32
50	42.61	36.64	31.27	26.98
60	45.73	39.87	32.11	26.76
70	46.12	42.38	36.12	30.33
80	48.6	45.31	38.64	32.95
90	51.93	46.83	41.82	35.76
100	54.17	48.47	41.63	34.45

The above Table 1 shows the comparison of peak signal to noise ratio for the proposed VSCS Method with the EMSBI method, AIRFT technique and APVQ method. It measures the capacity of the embedded secret data between soldiers in military to the bit rate which is obtained through the above table and increases gradually though linear conditions for different sizes provided by the sender soldiers. The experiments were conducted using different size of video frames ranging from 10 to 100 MB obtained from video quality experts group that measure the PSNR value.

Figure 7 illustrates the peak signal to noise ratio using EMSBI method, AIRFT technique, APVQ method and Proposed VSCS Method for visual comparison based on different stego message of different sizes. The low peak signal-to-noise ratio was recorded because of managing the noise ratio on the basis of the original coefficient values and embedded coefficient values.

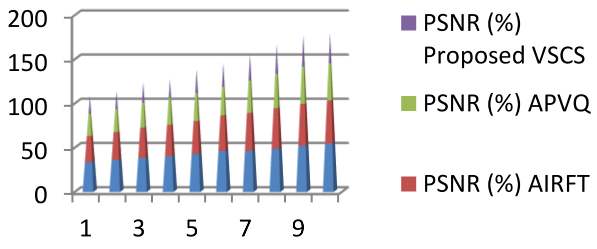

Figure 7. Comparison of PSNR for EMSBI, AIRFT, APVQ method and proposed VSCS method.

Besides, while increasing the sizes of video frames, the peak signal to noise ratio is also getting increased. Grade Reversible Adjoin Prediction mechanism is applied on the secret information to embed the data per pixel in that video frame. In the encoding side, an index value of secret data in each video frame is embedded to ensure that the secret data is recovered back with higher quality rate on the decoding side. Due to, by applying index value points for easily achieve the performance level on video code streams. The embed index value is decoded to the adjoining secret key of a state secret frame in the video frame to extract the secret information. Therefore, the peak signal to noise ratio using VSCS method is reduced by 49% when compared with APVQ. Similarly, the other EMSBI method and AIRFT technique reduce the peak signal to noise ratio by 13% and 27% hence, the proposed VSCS method provides better peak signal to noise ratio.

3.2. Security Level Based on Size of Secret Data

The robustness of the system is measured in terms of security of the hidden message sent and hidden message received. Higher the difference more securitized the method is said to be. It shows better capacity by organizing random video frames for hiding message.

$$\text{Security Level} = \frac{(\mathrm{HSD_S} - \mathrm{HSD_R})}{\mathrm{HSD_S}} * 100 \quad (3)$$

From Equation (3), HSD_S and HSD_R denotes the number of hidden data sent and received for video steganography. Higher the difference more securitized the method is said to be. It is measured in terms of percentage (%).

Table 2. Comparison of security level for EMSBI, AIRFT, APVQ method and proposed VSCS method.

Size of secret data (MB)	Security Level (%)			
	EMSBI	AIRFT	APVQ	Proposed VSCS
23.4	37.58	43.58	47.35	52.58
25.4	39.72	45.95	49.63	54.69
43.3	42.37	47.39	52.89	57.25
51.2	46.68	51.86	55.68	59.87
65.3	49.32	55.64	59.72	63.25
76.8	53.4	58.64	63.48	67.46
82.6	56.95	61.27	65.87	69.87
91.4	58.61	63.62	67.66	73.21
106.9	59.37	64.97	69.42	74.96
117.8	62.12	68.2	72.34	76.24

The above Table 2 shows the experimental values of the security level for the EMSBI method, AIRFT technique and APVQ method with the proposed VSCS method. Here, the size of the secret data is considered in the range of 23.4 KB to 117.8 KB using different images. The method is said to be more efficient, when the robustness of security is high. The security returned over other methods increases gradually though not linear for different sizes of secret data for which video steganography is observed.

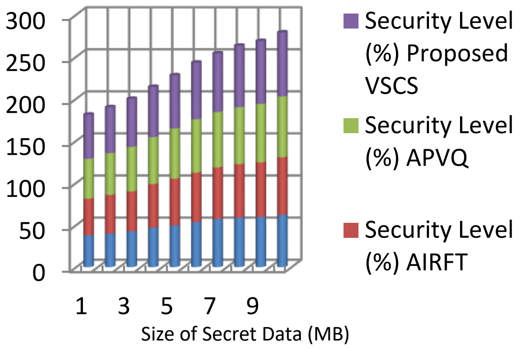

Figure 8. Comparison of security level for EMSBI, AIRFT, APVQ method and proposed VSCS method.

Figure 8 illustrates the security level using the EMSBI method, AIRFT technique and APVQ method and compared for visual comparison based on different sizes of secret data for video steganography. For example, when the size of the secret data was 23.4 KB, the security obtained was 37.58% using EMSBI method, 43.58% in AIRFT technique and 47.35% in APVQ method and in the proposed VSCS method 52.58%. By observing the large video frame with differing sizes of secret data for video steganography, the security is improved. In military services, different video frames are transferred between soldiers about battle field, military units, and secret information and so on. This is because with the application of Grade Reversible Adjoin Prediction, the secret messages are hidden and make it complicated for attackers to identify the prevalence of secret messages.

Therefore, the security level using VSCS method is improved by 24% when compared with APVQ. Hence, the proposed VSCS method provides better security level while communicating between the two different services.

3.3. Runtime with Respect to Size of Stego Messages

Runtime is defined as the measure of time taken to extract the stego messages with respect to the size of stego messages. It is measured in terms of millisecond (ms) and it is mathematically formulated as given below.

$$\text{Runtime (ms)} = \text{Extraction Time (Stego message)} * \text{ SMS} \quad (4)$$

From Equation (4), runtime is obtained based on the stego message size 'SMS'. Lower the runtime, more efficient the method is said to be.

The below Table 3 represents the runtime obtained using MATLAB simulator and comparison is made in the EMSBI method, AIRFT technique and APVQ method, with the proposed VSCS Method. Experimental evaluation of runtime is evaluated with the stego message size ranging from 23.4 KB to 117.5 KB.

Table 3. Comparison of runtime for EMSBI, AIRFT, APVQ method and proposed VSCS method.

Stego message size (KB)	**Runtime (ms)**			
	EMSBI	**AIRFT**	**APVQ**	**Proposed VSCS Method**
23.4	37.89	26.14	21.85	19.58
25.7	41.42	28.53	23.61	20.58
31.3	44.56	31.12	26.74	19.62
43.2	47.23	32.34	27.98	20.58
88.3	52.49	36.45	29.14	22.95
92.5	52.8	37.2	32.89	27.14
97.6	56.17	42.31	33.87	29.43
108.4	59.46	43.82	38.17	31.56
112.3	60.3	46.15	39.78	33.85
117.5	62.06	48.21	42.12	37.96

Figure 9 shows the variation of the runtime rate as a function of Internet Archive 501(c) (3), provided as input. Comparatively, the runtime observed is lower using APVQ method, the other EMSBI method and AIRFT technique compared with the proposed method VSCS respectively. The authentic acceptance rate at the receiving end is increased by using Video Region Match Vector Quantization.

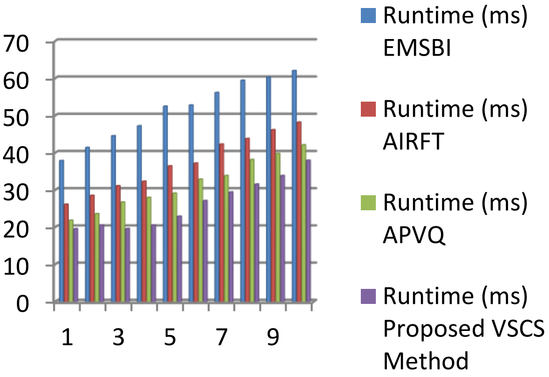

Figure 9. Runtime comparison for EMSBI, AIRFT, APVQ method and proposed VSCS method.

It efficiently decodes adjoining frames with index values with larger test samples. Moreover by integrating both the new pixel value and pixel region value, the reversible method potentially attains better quality of information with minimal runtime using the vector quantization. The APVQ method in turn decodes adjoining frames with index values with larger test samples resulting in minimizing the runtime to extract the stego message with respect to size of the stego message. Therefore, the runtime using VSCS method is minimized by 41% when compared with APVQ. Similarly, the EMSBI method and AIRFT technique minimizes the runtime value by 15% and 19%. Hence, it is proved that the proposed VSCS method provides better runtime while communicating the data between two different services.

4. Conclusions

In conclusion, the perfect illustrations are discussed on the analysis of the EMSBI method, AIRFT technique, APVQ method and VSCS Method. Initially, Enhanced bit irreversible method increases the efficiency of the embedded payload in video Steganography and maintains robustness on video code streams with minimum peak signal-to-noise ratio. Next, Secure polynomial hashing function provides minimum complexity of data hiding and attains the data randomness without information loss on the video frames. Next, Grade Reversible Adjoin Prediction mechanism is used for extracting an adjoining prediction on secret data. Finally, VSCS method applied for embedding secret data. Therefore, embedding and extraction on algorithm is applied with the region on interest which improves the efficiency of the video Steganography process.

Reference

[1] Aly H., "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, pp. 14-18, 2011.

[2] Aruna L. and Aramudhan M., "A Novel Survey on SLA based Load Leveling in Cloud Computing," *International Journal of Research in Computer and Communication Technology*, vol. 3, no. 6, 2014.

[3] Aung P. and Naing T., "A Novel Secure Combination Technique of Steganography and Cryptography," *International Journal of Information Technology, Modeling and Computing*, vol. 2, no. 1, pp. 55-62, 2014.

[4] Bedi P., Bansal R., and Sehgal P., "Using PSO in a Spatial Domain Based Image Hiding Scheme with Distortion Tolerance," *Computers and Electrical Engineering*, vol. 39, no. 2, pp. 640-654, 2013.

[5] Cogranne R., Retraint F., Zitzmannm C., Nikiforov I., Fillatre L., and Cornu P., "Hidden Information Detection using Decision Theory and Quantized Samples: Methodology, Difficulties and Results," *Digital Signal Processing*, vol. 24, pp. 144-161, 2014.

[6] Cogranne R., Zitzmann C., Retraint F., Nikiforov I., Cornu P., and Fillatre L., "A Local Adaptive Model of Natural Images for Almost Optimal Detection of Hidden Data," *Signal Processing*, vol. 100, pp. 169-185, 2014.

[7] Feng B., Lu W., and Sun W., "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 243-255, 2015.

[8] Ghuge S., Kumar N., Savitha S., and Suraj V., "Multilayer Technique to Secure Data Transfer in Private Cloud for SaaS Applications," *in Proceeding of the International Conference on Innovative Mechanisms for Industry Applications*, Bangalore, pp. 646-651, 2020.

[9] Gulve A. and Joshi M., "An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach," *Mathematical Problems in Engineering*, pp. 1-12, 2015.

[10] Kelash H., Abdel Wahab O., Elshakankiry O., El-sayed H., "Utilization of Steganographic Techniques in Video Sequences," *International Journal of Computing and Network Technology*, vol. 2, no. 1, 2014.

[11] Lin T., Chung K., Chang P., Huang Y., Liao H., and Fang C., "An Improved DCT-based Perturbation Scheme for High Capacity Data Hiding in H.264/AVC Intra Frames," *Journal of Systems and Software*, vol. 86, no. 3, pp. 604-614, 2013.

[12] Saha B. and Sharma S., "Steganographic Techniques of Data Hiding Using Digital Images," *Defence Science Journal*, vol. 62, no. 1, pp. 11, 2012.

[13] Shanableh T., "Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 455-464, 2012.

[14] Thahab A., "A Novel Secure Video Steganography Technique using Temporal Lifted Wavelet Transform and Human Vision Properties," *The International Arab Journal of Information Technology*, vol. 17, no. 2, pp. 147-153, 2020.

[15] Thai T., Retraint F., and Cogranne R., "Statistical Detection of Data Hidden in Least Significant Bits of Clipped Images," *Signal Processing*, vol. 98, pp. 263-274, 2014.

[16] Ulibrk D., Mirkovic M., Zlokolica V., Pokric M., Crnojevic V., and Kukolj D., "Salient Motion Features for Video Quality Assessment," *IEEE Transactions on Image Processing*, vol. 20, no. 4, pp. 948-958, 2011.

[17] Umadevi R. and Nasira G., "Video Steganography Based on Hash Polynomial Function for Secure Communication Use Fourier Transform with Security Method for Mounting of Multilayer Security," *Indian Journal of Science and Technology*, vol. 8, no. 23, pp. 1-4, 2015.

[18] Umadevi R., "Joint Approach for Secure Communication Using Video Steganography: Achieving Better Communication Based on Video Steganography," *in Proceeding of the International Conference on Computing for Sustainable Global Development IEEE Conference*, New Delhi, pp. 3104-3106, 2016.

[19] Wang W., Huang C., and Wang S., “VQ Applications in Steganographic Data Hiding Upon Multimedia Images,” *IEEE Systems Journal*, vol. 5, no. 4, pp. 528-537, 2011.

Umadevi Ramamoorthy a post graduate in Information Technology and Management from Kongu Engineering College, Perundurai, has completed her M.Phil in Computer Science and Ph.D in Computer Science at Periyar University, Salem and presently working as Assistant Professor and Head in Computer Science and Application in Vivekanandha College for Women, Unjanai. With 15 years of teaching experience. She has been presenting and published papers in several International and National Conferences and journals. She is a member of the CSI, and IAENG. She has published patent by Intellectual Property, Government of India.

Aruna Loganathan a post graduate in Computer Science from Jamal Mohamed College, Tirchy, has completed his M.Phil in Comiddenputer Science in St. Joseph's College,Trichy and Ph.D in Computer Science at Periyar University, Salem and presently working as a Professor in CS & Principal in Vivekanandha College for Women, Unjanai. With 26 years of teaching experience he has been presenting papers in several International and National Conferences. He has produced 26 Research Scholars in M.Phil Computer Science and as on date, a member of the CSI. ISTE, IACSIT and IAENG. He sincerely believes that his maiden venture will bring a scholarly recognition from veterans of the field.