International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor (2018): 7.426

Secure Data Transmission of Video Steganography by Hashing Pixel Values with DWT

Hnin Lai Nyo[1], Aye Wai Oo[2]

[1, 2]Fauluty of Information and Communication Technology, University of Technology (Yatanarpon Cyber City), Pyin Oo Lwin, Myanmamr

Abstract: ***The growing possibilities of modern communications need the high security especially on computer network. Due to the increasing number of data being exchanged on the internet, it is becoming more important to the network security. Therefore, the confidentiality and data integrity are required in order to protect against unauthorized access and use. This has caused to the emergency growth of information hiding research area. In this system, combination of steganography and cryptography techniques are used to transmit data securely to the authorized person and to improve imperceptibility and payload capacity. The hashed frequency values of secret image are embedded in the video file with the use of Discrete Wavelet Transformation and Least Significant bit. The secret key generated these hashed values is encrypted with the another secret key by using a new encryption algorithm, Twisted Exchange Algorithm and the resulted encrypted key is hide behind the audio file with the parity bit technique. The system performance is measured MSU video quality measurement tool and the results are analysed with different parameters.***

Keywords: cryptography, steganography, security, discrete wavelet transform, least significant bit

1. Introduction

Now a days as the use of internet increase, providing security to the information is also important thing. Providing security means protection information systems form unauthorized access, use, disruption, modification and recording or destruction. There are two methods to provide security. When it is used the internet as a medium to access desired information, the attackers or the more secure transmission of confidential data becomes a great deal of attention. Many techniques such as digital watermarking, steganography and cryptography are used to improve the security of data. Steganography is the art and science of concealing information in such a way that only the sender and the user that can only receive a secret message should be aware of its presence. Thus, a stego system aims to reduce any suspicion that a third party may have over occurring communication. Recent research interest towards steganography focuses primarily on applications in the digital domain. Modern digital stego system embeds data through a variety of data hiding techniques such as image, audio and video steganography. Among them, video steganography becomes a rising interest area because the pervasive nature of video, along with an increased embedding capacity, make it and ideal candidate**.** Cryptography, in which information is allowed to be sent in a secure form and the only intended receiver able to retrieve this information. Its main purpose is not only to provide confidentiality, but also to provide solutions for other problems such as data integrity, authentication, non-repudiation. So that, combination of steganography and cryptography also provides a higher security level, robustness, imperceptibility and payload capacity. Therefore, the proposed system uses this combination of steganography and cryptography technique**.**

2. Related Work

Ramadhan J. Mstafa', Khaled M. Elleithy' and Eman Abdelfattah [1] proposed a robust and secure video stenographic algorithm in discrete wavelet transform (DWT) and discrete cosine transform (DCT) domains based on the multiple object tracking (MOT) algorithm and error correcting codes. The secret message is preprocessed and to distinguish the regions of interest in moving object, motion-based MOT algorithm is implemented. Then, the secret data is hide into the DWT and DCT coefficients of all motion regions in the video depending on foreground masks. As the experimental results, it gives the higher PSNR values from other method so that this system improve embedding capacity, imperceptibility, robustness and security. A. Swathi, Dr. S.A.K Jilani [2] also expressed a video steganography method in which the LSB substitution using polynomial equation is developed to hide the information in specific frames of the video. The text data is embedded based on the key and the key is in the form of polynomial equations with different coefficients. Thus, this method increases the capacity of embedding bits into the cover image. Ashawq T. Hashim, Dr. Yossra H. Alii & Susan S. Ghazoul [3], stated a combination of steganography and cryptography technique. In order to increase the level of security and to make the system more complex to be defeated by attackers, the AVI file is separated into two parts: video and audio file. The secret message is embedded into the video and the key is hide in audio. Cryptography method, Blowfish algorithm is also used. According to the test results, it produces good results for PSNR (above 50db). M.AI-Hazaimeh Obaida [4] proposed symmetric key based new video steganography algorithm. It splits the selected video into audio samples and video frames. Next to generate public key, it uses the audio sample. Along with this key it encrypts the yielded audio sample and video frame in order to produce the cipher data. Then it randomly adds the public key to the cipher data. At receiver side, the public key from the cipher is firstly extracted and the remaining decryption process is continued completely. It showed that PSNR values (between 30 and 58dB) and MSE values (close to zero) as the high performance. Abhinav Thakur, Harbinder Singh, Shikha Sharda [5] showed data hiding technique in which the secret data is embedded into the cover video. In this system, firstly the cover video is decomposed into different frames and the secret data is scrambled with Arnold scrambling

technique and this resulted data is transformed by single level discrete wavelet transform method. The cover file is also transformed with DWT and embed the secret data into the blue channel of the cover with the use of alpha blending method. Therefore, this results highly secure with good perceptual invisibility.

3. Methodology of the System

Steganography supports lack of versatility with respect to its cover file format and data file format and can carry the large amount of data. However, security layers are not added effectively which results in insecure communication. This system combines both cryptography and steganography in order to provide higher level of security, imperceptibility, payload capacity. Thus , to ensure the secret message (image) arrives to the intended receiver, double key encryption method is used. For the key encryption and decryption process, stream cipher based Twisted Exchange algorithm is used. It provides fast communication speed and more secure system because it uses multiphase operations and its generated key streams are randomness and unpredictability. As the embedding process of the system, the secret message (image) is embedded into the cover video by hashing its pixel values with the use of constant value and secret key. And this secret key is hide behind the audio file. However, before embedding this secret key, it is encrypted with another secret key (pre-shared key) by stream cipher based Twisted Exchange Algorithm. The pre-shared key is the key that must be known by both the sender and receiver. So that, the system is divided into two parts; one is encryption processes (sender side) and the other is decryption processes (receiver side). The detail information of these parts explain as the following.

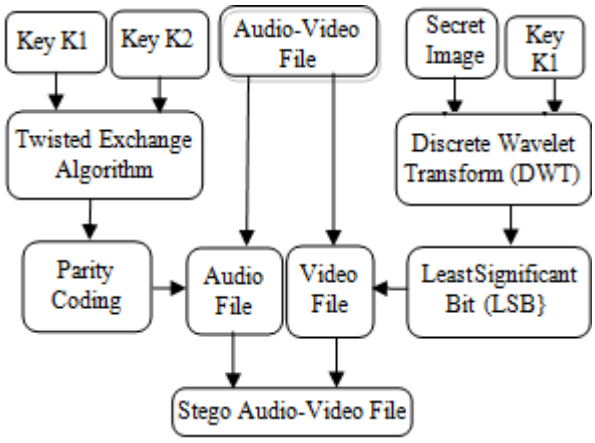

Figure 1: Encryption Processes (Sender Side)

3.1 Encryption Processes (Sender Side)

In the encryption processes, in which the system user, sender selects any one audio-video file and then this file is separated into individual audio and video file which is a collection of multiple frames. And the sender chooses the separated video file and a secret image which will be transmitted to the receiver. Before hiding the secret image behind the video file, it is transformed spatial domain to frequency domain by discrete wavelet transform (DWT) method. The resulted frequency values is decomposed into the three hashing values with the use of secret key (key K1) and constant value. The three referable frequency values are embedded into red, green and blue (RGB) channel of the selected frame by applying least significant bit (3,4,4LSB) technique[6]. The selected frame may be any number that the sender want. The following equation (1), (2) and (3) are used to embed the hashed frequency values of the secret image into the three R,G,B channel of the selected frames in cover video file. After embedding the secret image behind the video file, it becomes a stego video file. And then, the system also wants to provide higher level of security for it, double key encryption method is used. It means that the first secret key (key K1) used for embedding the secret message (image), is encrypted with the another secret key (key K2) by stream cipher based Twisted Exchange algorithm. Then, the generated encrypted message and selected frame number are hided into the audio file by using parity coding technique [7] as stego audio file. Finally, these two stego video file and stego audio file are combined into one stego audio-video file and send this stego file to the intended receiver through the internet. The above figure (1) shows the encryption processes of the system.

$$B = F / K \quad (1)$$

$$R = (F \% K) / n \quad (2)$$

$$G = (F \% K) \% n \quad (3)$$

Where, R,G,B means red, green and blue channel of the cover video frame, F is frequency values of the secret image, K is the secret key and n is the constant number used in this system.

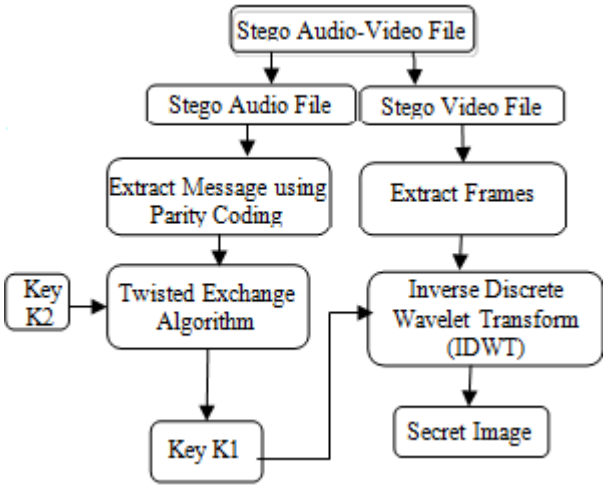

Figure 2: Decryption Processes (Receiver Side)

3.2 Decryption Processes (Receiver Side)

In the decryption processes of the system (receiver side) shown in figure (2), receiver selects the stego audio-video file sent from the sender and it is separated into individual stego audio and stego video file. To retrieve the secret message (image) sent from the sender, firstly the receiver must choose stego audio file and extract the message and selected frame number in it by using parity coding technique. And, the message is decrypted with secret key (key K2) that is known both the sender and receiver by using Twisted Exchange algorithm. Then the generated decrypted message that means the secret key (key K1) and frame number are used to extract the secret message (image) embedded in the stego video file. The hashed frequency values are extracted

from the R,G,B channel of the generated frame number and these values convert to original frequency values by using the secret key (key K1). It is expressed in the following equation (4). Next, with the use of inverse Discrete Wavelet Transform (IDWT), the original secret message (image) is rebuild from these frequency values. As this way the secret image is received securely and secretly by the receiver.

$$F = (B * K) + ((R * n) + G) \quad (4)$$

4. Experimental Results of the System with MSU Tool

Since the essential goal of steganography is the concealing of the fact that a secret message is transmitted, then it is very important to make the stego-video to be as close as to the cover-video. In fact, imperceptibility of the stego AVI reflects how much it is affected due to embedding process, in other words, imperceptibility can be decided by measuring that effect. In the proposed system, the MSE and PSNR measurements as shown in equation (5),(6) are adopted. MSE is one metric used to assess how well a method to reconstruct an image performs relative to the original image. It shows mean square error for two images or frames [9].

$$d(X,Y) = \sum_{i=1}^{m}\sum_{j=1}^{n}(X_{ij} - Y_{ij})^2 / mn \quad (5)$$

$$PSNR = 10\log_{10}(MaxErr^2 * m * n / \sum_{i=1}^{m}\sum_{j=1}^{n}(X_{ij} - Y_{ij})^2 \quad (6)$$

Table 1: Results of MSE and PSNR of original and stego video frame

Secret Image (size)	Cover video (size)	Frame No.	MSE	PSNR
E1.jpg (225*259)	nat.avi (264*352)	96	5.4915	41.5373
	urscent.avi (360*640)	91	3.0466	43.5480
	novo.avi (720*1280)	78	4.4442	41.6770
Lena.jpg (256*256)	nat.avi (264*352)	80	8.9896	39.4613
	urscent.avi (360*640)	72	8.0528	39.8273
	novo.avi (720*1280)	46	52.19	30.9545
Chilli.jpg (512*512)	nat.avi (264*352)	52	10.4749	38.7861
	urscent.avi (360*640)	89	8.8674	39.3529
	novo.avi (720*1280)	59	20.5057	35.0178
Medical.jpg (768*578)	nat.avi (264*352)	34	9.5085	39.2731
	urscent.avi (360*640)	24	8.7169	39.5581
	novo.avi (720*1280)	35	10.9012	37.7578
Love02.jpg (1024*768)	nat.avi (264*352)	63	8.2067	39.9318
	urscent.avi (360*640)	48	6.9196	40.2879
	novo.avi (720*1280)	112	61.7741	30.2290
Map.jpg (1280*720)	nat.avi (264*352)	116	8.9274	39.5908
	urscent.avi (360*640)	101	9.1469	39.2771
	novo.avi (720*1280)	98	12.2742	37.5023
Burma.jpg (430*547)	nat.avi (264*352)	121	6.8385	40.3990
	urscent.avi (360*640)	65	8.74	39.7021
	novo.avi (720*1280)	90	5.6044	40.7201

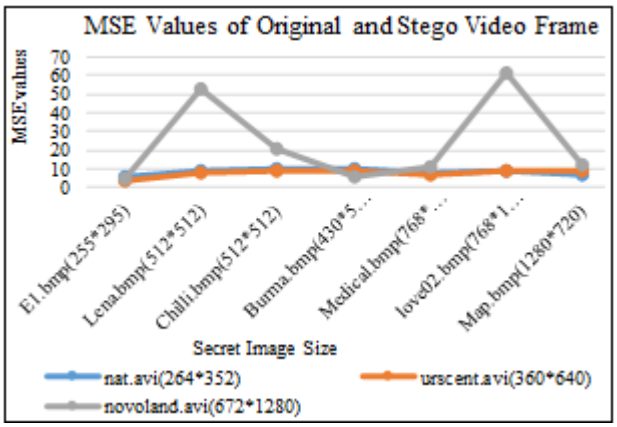

Figure 3: Comparison of MSE Values of original and stego video frame with embedding different images into different video quality files

The above table (1) shows the testing results of MSE and PSNR values of original video frame and stego video frame of different quality video file such as nat.avi (263*352), urscent.avi (360*640) and novo.avi (720*1280) by embedding variable image size. According to the table (1), even low quality video file, nat.avi(264*352) gives its PSNR values (40db and over 40db) as any other high quality video file if it compares its original video frame. As an overall performance of the system between original and stego video frame, it supports satisfied PSNR values that is over 40db. Next, figure (3) and (4) also express MSE and PSNR values of this table results as char types. The three R,G,B channel histogram of original video frame and stego video frame in which embeds a secret image is shown in figure (5) and (6). It is found that the histograms of original and stego video frame are same. And then, figure (7) and (8) show the comparison resulted values of original secret image and extracted secret image from embedding different secret image size into different video quality files. Also their same histogram results are shown in figure (9) and (10).

5. Conclusion

The system is secure video steganography method using discrete wavelet transform (DWT) and combination of cryptography based. In order to provide more security, the preprocessing stage of secret image and double key encryption processes is used. To authenticate the intended

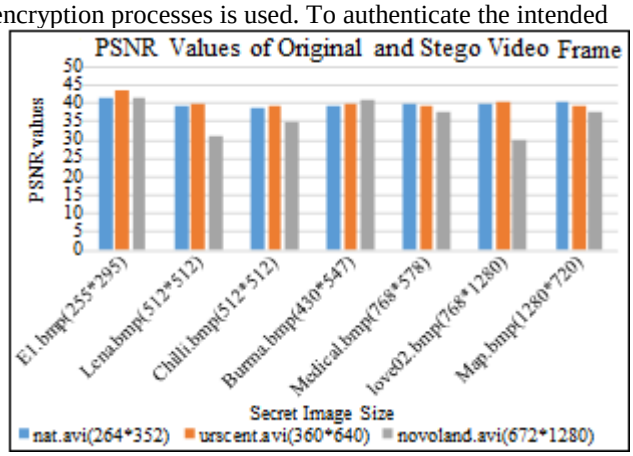

Figure 4

Figure 4 is Comparison of PSNR Values of original and stego video frame with embedding different images into different video quality files

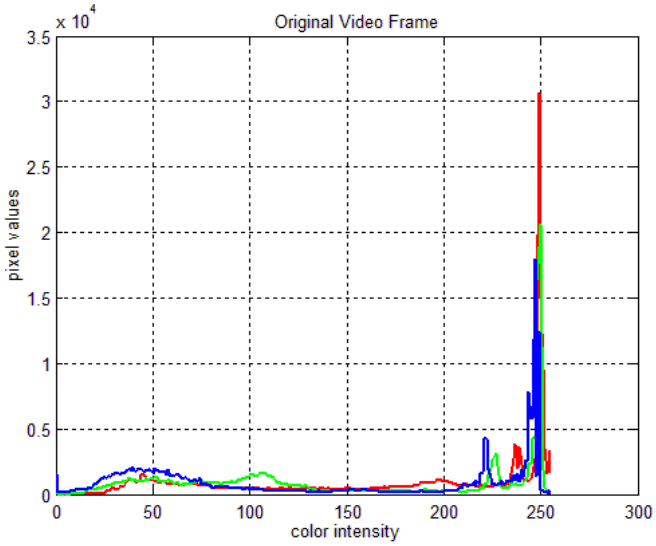

Figure 5: R,G,B channel histogram of original stego frame number 48 in original urscent.avi

user receives the information sent, a pre-shared key is also applied. And then, frequency values of secret image is hashed and the resulted hashing values are embedded diffusely in the video file. Moreover, the secret key generated these hashing values is encrypted before embedding behind the audio file. In this paper, the performance of the system is also tested and analyzed using MSU video quality measurement tool. In summary, according to the above analysis results, the system can support a higher security level, payload capacity and imperceptibility to the users securely and safely.

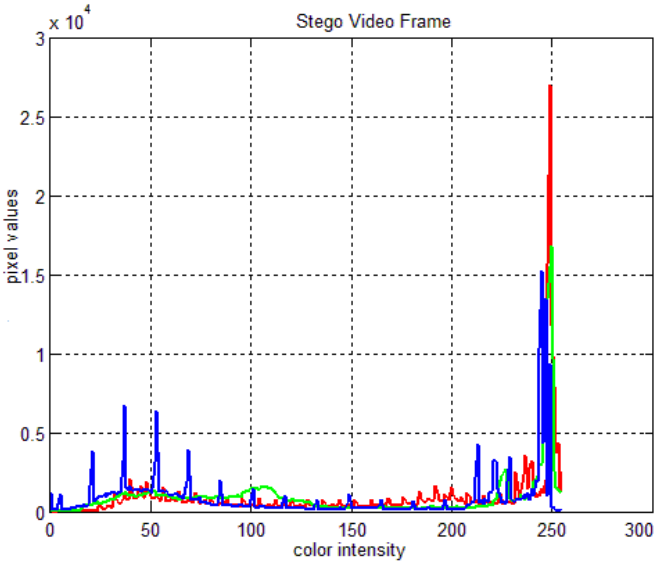

Figure 6: R,G,B channel histogram of stego video frame number 48 in stego urscent.avi file

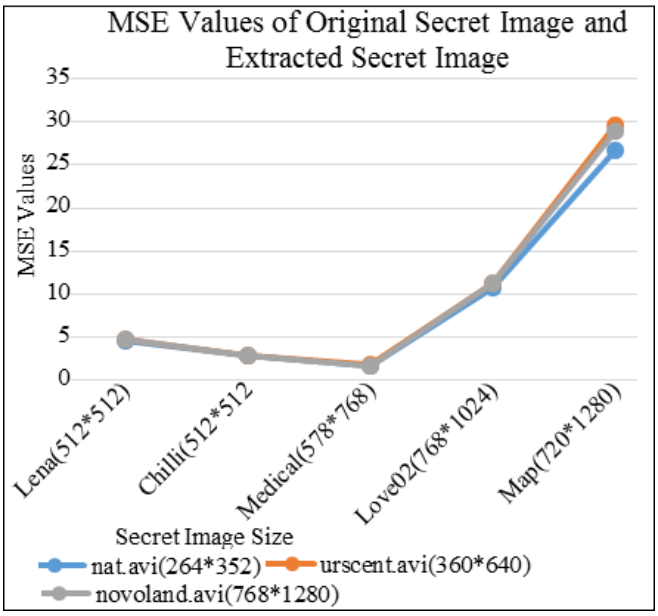

Figure 7: Comparison of MSE values of original and extracted secret image from different video quality files

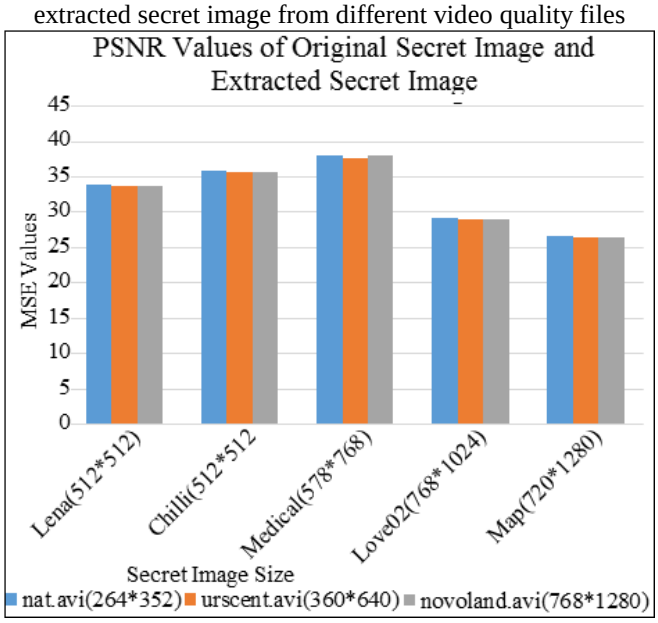

Figure 8: Comparison of PSNR values of original and extracted secret image from different video quality files

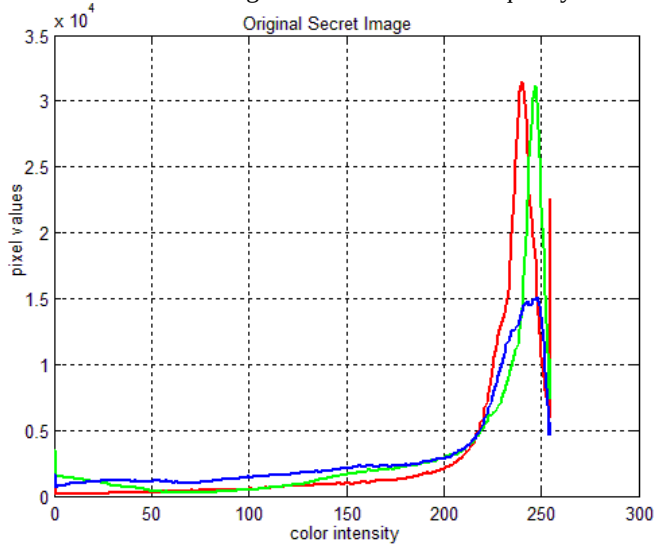

Figure 9: R,G,B Channel Histogram of Original Secret Image

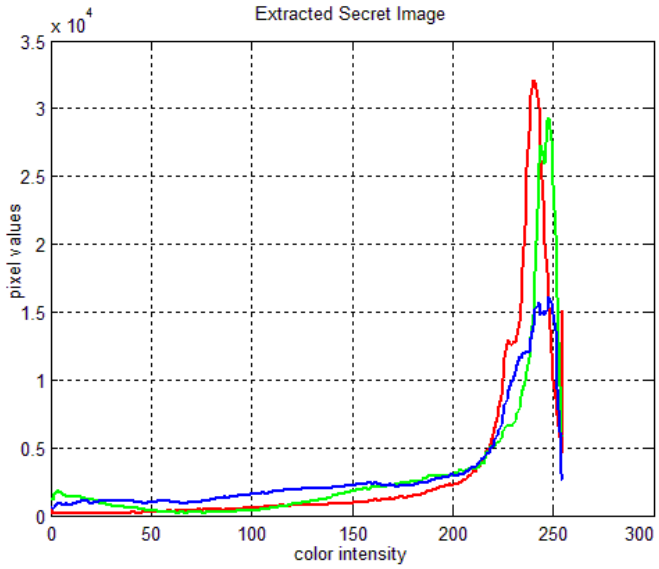

Figure 10: R,G,B Channel Histogram of Extracted Secret Image

References

[1] Ramadhan J. Mstafa', Khaled M. Elleithy' and Eman Abdelfattah,' A Robust and Secure Video Steganography method in DWT-DCT Domains based on Multiple Object Tracking ECC", Digital Object Identifier 10.1109/ACCESS.2017.2691581, May 17, 2017.

[2] A.Swathi 1, Dr. S.A.K Jilani,"Video Steganography by LSB Substitution Using Different Polynomial", national Journal of Computaional Engineering Research (ijceronline.com) Vol.2. Issue.5.

[3] Ashawq T. Hashim, Dr. Yossra H. Alii & Susan S. Ghazoul, "Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganography", Eng. & Tech. Journal, Vol.29, No.2, 2011

[4] M. AI-Hazaimeh Obaida, "Combining Audio Samples and Image Frames for Enhancing Video Security", Indian Journal of Science and Technology, Vol 8(10), 940–949, May 2015

[5] Abhinav Thakur, Harinder Singh and Shikha Sharda "Secure Video Steganography based on Discrete Wavlet Transform and Arnold Transform", International Journal of Computer Applications (0975 – 8887) Volume 123 – No.11, August 2015.

[6] K.Parvathi Divya and K. mahesh, "Various Techniques in Video Steganography- A Review", International Journal of Computer & Organization Trends- Volume 4 Issue 1 January to February 2014.

[7] Jayaram P and et al, "Information Hiding Using Audio Steganography-A Survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[8] MSU video quality measurement tool, Availabe: http://www.compression.ru/video/quality_measure/vqmt_pro.html