I. J. Computer Network and Information Security, 2019, 6, 45-53
Published Online June 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.06.06

Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT

Hnin Lai Nyo
University of Technology (Yatanarpon Cyber City), Pyin Oo Lwin, Myanmar
E-mail:hninlai.1988@gmail.com

Aye Wai Oo
University of Technology (Yatanarpon Cyber City), Pyin Oo Lwin, Myanmar
E-mail: ayewaioo@gmail.com

Received: 27 March 2019; Accepted: 24 April 2019; Published: 08 June 2019

***Abstract*—**For the sensitive information, the best privacy demand must be supported in commercial, technical and legal regulations. In this system we used combination of steganography and cryptography techniques in order to improve imperceptibility, robustness, payload capacity and to transmit data securely. As the preprocessing step, Arnold scrambling and discrete wavelet transform (DWT) techniques are used over the secret image. Then the referable values are calculated from the values of transformed secret image with the use of a secret key and embed these referable values in the video file by least significant bit (LSB) technique. Moreover, the secret key is encrypted with a pre-shared key by a new stream cipher Twisted Exchange Algorithm. And the result encrypted message is embedded behind the audio file by Parity coding technique. As the experimental results, performance of the system is tested with different real time images and various video quality files and measured by different parameters (PSNR, MSE), then it is also analyzed with attacks.

***Index Terms*—**Security, Cryptography, Steganography, Arnold Scrambling, DWT.

I. Introduction

Today data security is main concerned in many areas: trusted third party to maintain the database, strong encryption technique and secure communication channel because of a challenging issue of data communication. Due to more rapid development in information technology, it is necessary to support the more secure transmission of confidential data. Thus, confidentiality and integrity of data from unauthorized users is basically made in this system. To enhance data security, steganography, cryptography and watermarking techniques were developed in many years ago. These techniques are also tried to develop and used by the terrorists. Also the government needs to promote more secure system with different data hiding methods. Cryptography is visible for the attacker to access the content of the cipher message and steganography is also easy to detects that a secret message presents in the stego file without security. By combination of these two techniques, it supports covering of each weakness and will enhance the security of embedded data [15]. Steganography aids secure information delivery goal without knowing unauthorized users and stenographic method such as video steganography have larger capacity for embedding and the degradation of video quality can't be observed by naked eyes. And cryptography helps the intended recipient to be able to retrieve the information, thus it provides security services such as confidentiality, integrity and authenticity. Therefore, in this system, a combination of steganography and cryptography is used to provide a higher security level, imperceptibility, robustness, and payload capacity.

II. Related Work

Ashawq T. Hashim, Dr. Yossra H. Ali & Susan S. Ghazoul [1], stated a combination of steganography and cryptography technique. This technique aims to increase security level and to make more complex system to be defeated by attackers. The input audio-video file is split into two parts: video and audio file. Then 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 testing results, it produces good PSNR results (above 50db) between cover and stego cover file. Praveen. P and Arun. R [2], proposed a method which is an audio-video crypto steganography system using advanced chaotic algorithm. It aims that the secret information is hide behind image and audio behind video file by using LSB substitution method. Advanced chaotic algorithm is used to decrypt and encrypt of data and images. PSNR and histograms are applied as parameters of security and authentication and the system

produces its PSNR value between the original and encrypted image range from 10 to 40db. Sadik Sli AI-Taweel, M. Husain AI-Hada and Ahmed Mahmoud Nasser [3], expressed a method in which an image to be encrypted with Arnold scrambling technique and hided in another image by least significant bit (LSB). Their method is tested various attacks and indicated that the algorithm provides good security and imperceptibility in gray images. Sghaier Guizani and Nidal Nasser [4], showed an optical crypto technique with adaptive steganography (AS). In this paper the intended audio/video sequences is encrypted and decrypted by the asymmetric encryption method, and it also uses double random phase encoding algorithm. Its aim is to hide the information within the cover media as much as possible. As its simulation results, it provides over 20dB of the conventional technique's PSNR values. Therefore, it concluded that their proposed scheme is more visual quality and data embedding capacity than the conventional technique. Prof. D. J. Bonde and et al [5] proposed combination of audio and video steganography using anti forensics techniques. To hide the secret image in the video file, forbidden zone data hiding (FZDH) is used and to hide text in audio file, phase coding algorithm is used. As the preservation of security, it matches the PSNR and histogram matching processes of receiver and sender. Rambabu Mudusu, A. Nagesh, M. Sdanandam [6] stated a mix of image steganography associated sound steganography. LSB technique is used to shroud the beneficiary's face image of video and the mystery information behind the audio. RSA algorithm is also applied for encryption of mystery information. For confront acknowledgment PCA is utilized and the confront verification procedure is completed to cross check the security parameter.

III. Methodology of the System

Steganography supports lack of versatility with respect to its cover and data file format and the large amount of data can be carried. However, it doesn't add security layers effectively which results in insecure communication. In order to provide higher level of security, imperceptibility, payload capacity, this system is combined both cryptography and steganography. Moreover, double key encryption method is also used to ensure that the secret message (image) is securely arrived to the intended receiver. For the key encryption and decryption process, it uses Twisted Exchange algorithm based on stream cipher. Twisted Exchange algorithm 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 number 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 processes of the system are expressed in the following two parts.

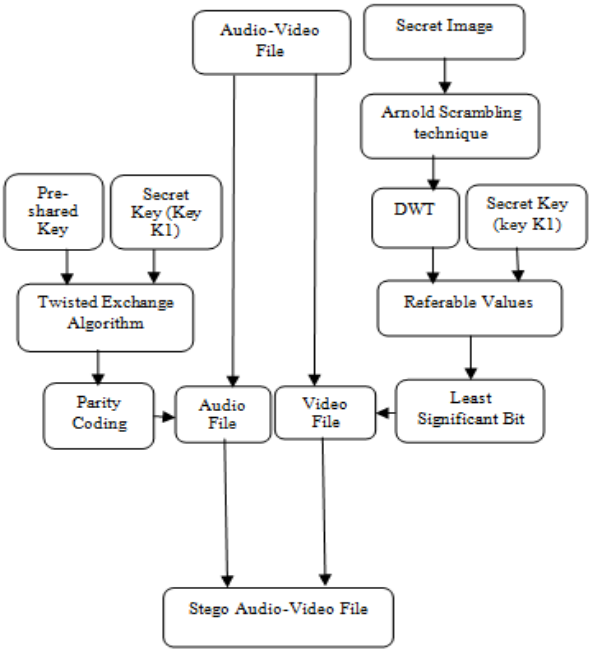

Fig.1. Embedding processes (Sender side) of the system

A. Embedding Processes

In the embedding processes (sender side), the user selects one video file which contains both audio and video. Then it is separated into individual audio file and video file. Then he/she chooses a video file and a secret image which will be transmitted to the intended user. The selection of frame to embed the secret image depends on the sender. As the preprocessing step, the secret image is scrambled by Arnold scrambling technique [13]. Although Arnold scrambling technique can access only square image, but this system can access any size of secret image by using this method with dividing multi-level square images from non-square image. Then, the scrambled image is transformed into four frequency values such as one approximation values and three details values by discrete wavelet transform (DWT) [11]. The referable values are calculated from these frequency values of secret image by using a secret key (key K1). Equation (1), (2) and (3) are used for the referable values calculation. And these referable values are embedded into the three channels (red(R), green(G) and blue(B)) of the selected frame by applying least significant bit (LSB) coding technique [7, 14], so it forms a stego video file. Next, the first secret key (key K1) is encrypted with a pre-shared key by Twisted Exchange algorithm. The pre-shared key means that both the sender and receiver must be known. Then the encrypted result message is hide behind the audio file with the use of parity coding technique [8] and it becomes a stego audio file. Lastly,

both the stego video file and the stego audio file are merged into stego audio-video file. Fig 1 shows all of the embedding processes.

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

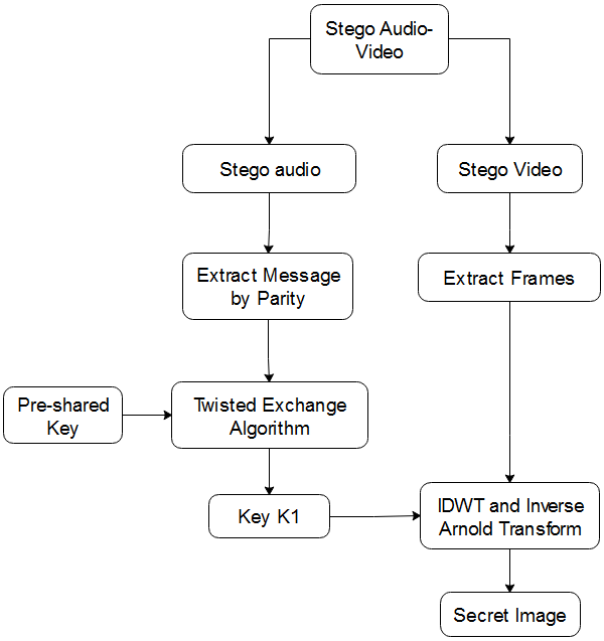

Fig.2. Extracting Processes (Receiver side) of the system

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

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

Where, R,G,B are the red, green and blue channel of the cover video frame, K is the average secret key and n is a constant number.

B. Extracting Processes

In the extraction processes (receiver side), the receiver selects the stego file and separates into stego audio and stego video file. If the receiver want to extract the secret image, firstly he/ she must select the stego audio file and uses a pre-shared key (key K2) to extract the first image secret key (key K1). By the time decryption of Twisted Exchange algorithm with the use of the pre-shared key (key K2), the system produce the embedded start frame number and the first secret key (key K1). Then the resulted key K1 and the embedded frame number are also applied to change referable values to frequency values as shown in (4). And these frequency values are inverse transformed by inverse discrete wavelet transform and inverse Arnold scrambling technique. Finally the system produces the original secret image sent from the sender to intended receiver securely and secretly. The whole extraction processes is shown in the above fig. 2.

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

C. Twisted Exchange Algorithm

Stream cipher algorithm is being widely used in information processing applications. For providing the confidentiality of different networks, kind of cryptography, stream cipher is applied. It is also symmetric encryption primitives [10]. Twisted exchange algorithm is based on stream cipher model with the use of pseudorandom number generator and its processing speed is fast. The life of stream cipher is key generation step, so its generated key stream must be random [16]. If the generator produces non-random key stream, the intruder or unauthorized user can predict or analyze the secret message. Therefore, in order to produce random key stream this algorithm consists of random exchange and multiphase operations. Generally, Twisted Exchange algorithm is divided into three parts: seed generation, key stream generation and plain text or cipher text production. Fig. 3 shows the general block of this algorithm. According to the system, in the seed generation part, a seed is generated from the user's image secret key. After that beginning with this seed, random key stream is generated as long as the length of plain text or cipher text. Finally, the generated random key stream and plaintext(cipher text) are encrypted (decrypted) to produce cipher text (plain text). These processing steps of algorithm are expressed in the following fig. 4.

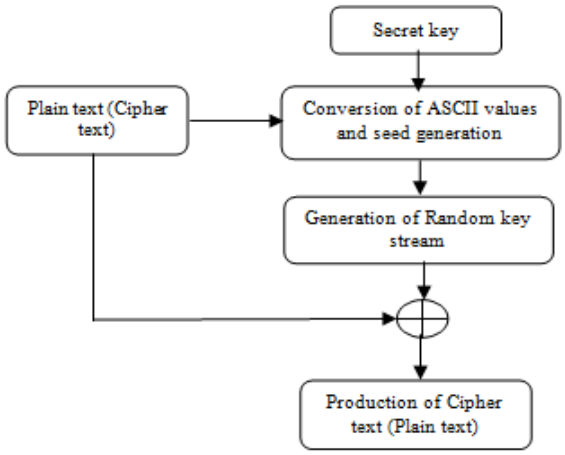

Fig.3. General block diagram of Twisted Exchange Algorithm

Step1: Seed Generation

1.1 Convert ASCII values of plain text / cipher text & secret key

1.2 for i=1 to length of secret key

seed= ASCII (x_i)*i ;

end

Setp2: Random Key Stream Generation

2.1 for i=1 to length of plain text / cipher text

2.1.1 Calculate two new values using seed

2.1.2 Execute xor with received two new values

2.1.3 for i=1 to 4

2.1.3.1 Convert 8 bits binary and exchange random two pair bits.

2.1.3.2 Perform xor with exchanged result and one of new value.

2.1.3.3 Calculate modulation of above result by 256.

2.1.3.4 Subtract the result from 255.

end

2.1.4 Perform xor the result and one of new values.

2.1.5 Modulate the addition of above result and i with 256.

2.1.6 Subtract the result from 255.

2.1.7 Produce key stream and seed

end

Step3: Plain text / Cipher text Production

3.1 Execute xor operation with each of key stream and plain text / cipher text

3.2 if most significant bit of the above result is one

3.2.1 Execute again xor operation the result and 255.

else

3.2.2 Execute xor operation the result and zero.

end

Fig.4. Twisted Exchange Algorithm

IV. Experimental Results

Steganography is the concealing of a secret message sent from the one to another, thus the stego file must be as close as to the cover-file. Mean Square Error (MSE) is how much the stego file is similar to the original file. The smaller its result value, the better its similarity quality. It is expressed in (5) and in which, X_{ij} is the pixel values of original image and Y_{ij} is the pixel values of stego image. m and n are rows and columns of the image. Imperceptibility of the stego file is affected due to embedding process and to evaluate the imperceptibility of the stego file, peak signal-to-noise ratio (PSNR) statistical test is used [9, 12]. PSNR is a standard measure to test the quality of the stego file. The larger its result values, the better its quality. It can be found in (6) and for eight bits image, the value of *MaxErr* is 255 [17]. In this section, some experiments are carried out to demonstrate the efficiency of the proposed method without and with attack. Then various size of secret image and various video quality files are used in real time. attack. Then various size of secret image and various video quality files are used in real time.

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

$$PSNR = 10\log_{10}(MaxErr^2 / MSE) \quad (6)$$

For the experiment of the system, various sizes of secret images such as Rose.jpg (240*300), Skull.jpg (366*630), Lena.jpg (512*512), Pepper.jpg (512*512), Abdomen.jpg (768*578), Map.jpg (724*1024) and love02.jpg (768*1024) are used for hiding in different video quality files (Nat.avi (264*352), Urscent.avi (360*640), Novoland.avi (678*1280), Utook.avi (720*1280)). In fig. 5 and fig. 6, MSE and PSNR results between original video frame and stego video frames of Urscent.avi video file. In which, each of the above secret images are embedded in a video file (Urscent.avi) and saves individual stego video file. Then embedded video frames of each stego video file and the original video frames are evaluated by the above equations: (5) and (6). In the invisibility of benchmark, acceptable PSNR value is 30db, therefore, according to the tested results, it is found that PSNR values of original and stego video frames have 35db and more. After that, each of these various size of secret image is also embedded in other different video quality files such as Nat.avi, Novoland.avi and Utook.avi. All of tests result for these different video file are also shown in fig. 7 and fig. 8. In these tests, whenever any size of secret image is embedded in any video quality file, the system provides its imperceptibility of PSNR values at least 35db. Hence, it supports acceptable and satisfied result for the users.

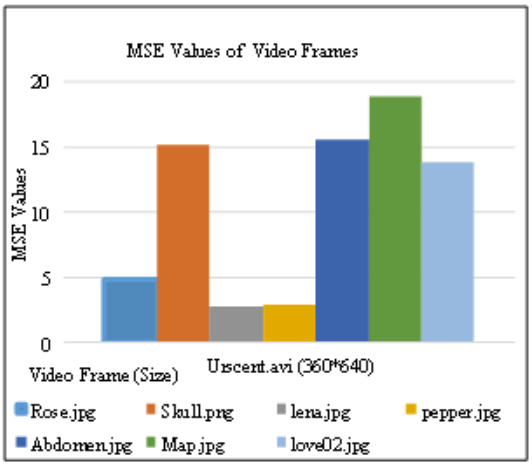

Fig.5. MSE Results for Original and Stego Video Frame of Urscent.avi

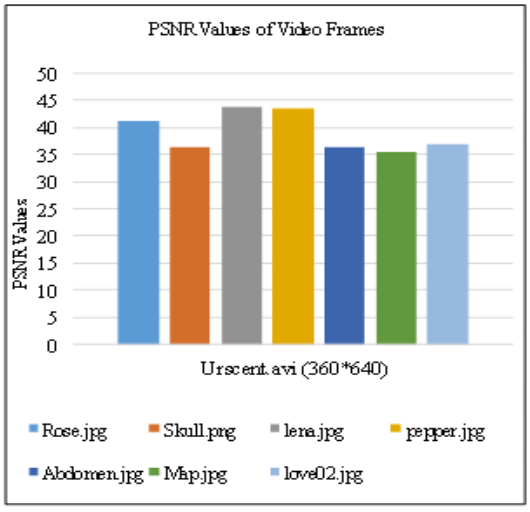

Fig.6.PSNR Results for Original and Stego Video Frame of Urscent.avi

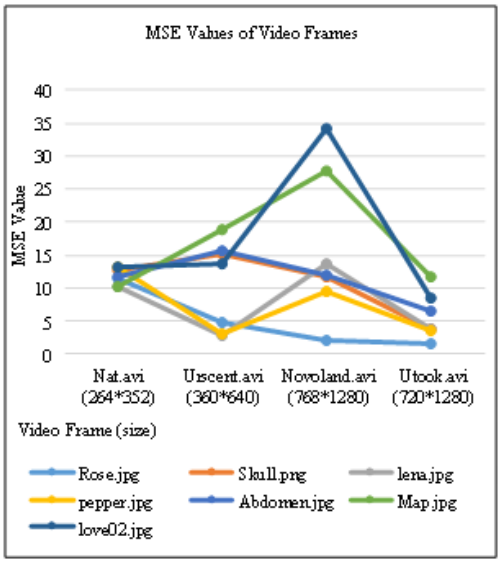

Fig.7 MSE Results for original video frames and stego video frames of different video quality files

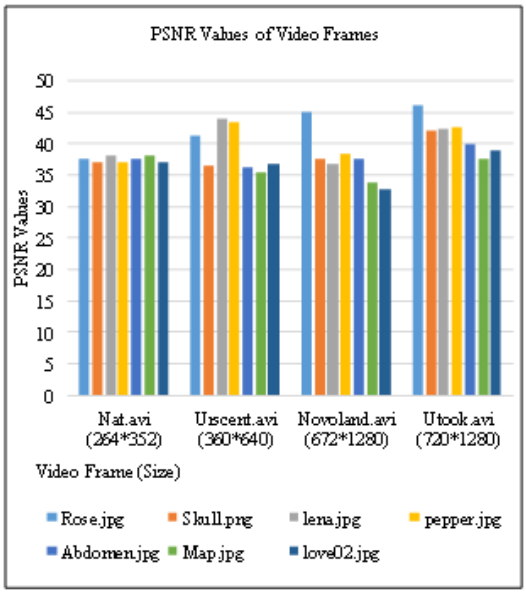

Fig.8. PSNR for original video frames and stego video frames of different video quality files

Also in the fig. 9 and fig. 10, it expresses the statistical test of MSE and PSNR values between original secret image and extracted secret image from embedded video file (Urscent.avi). In which, each secret image: Rose.jpg, Skull.jpg, Lena.jpg, Pepper.jpg, Aabdomen.jpg, Map.jpg, Love02.jpg is hide in a video file and these embedded secret images are extracted from stego video file. Then when the extracted secret images are compared with the original secret images, it can be found that PSNR results of secret images are over 24db and more even poor resolution image. Moreover, this type of experiment is also tested with different resolution video files: Nat.avi, Novoland.avi, Utook.avi and evaluate its MSE and PSNR values. These results are shown in fig. 11 and fig. 12. As its testing results, whenever any size of secret images are embedded in any resolution video file, the correct secret image's size can be extracted and even poor quality video file produces 24db and over of PSNR values. Acceptable value of secret message in PSNR is 20db, hence because the system supports at least 24db of satisfied PSNR value for the extracted secret image, it can be advantage for the convert communication persons.

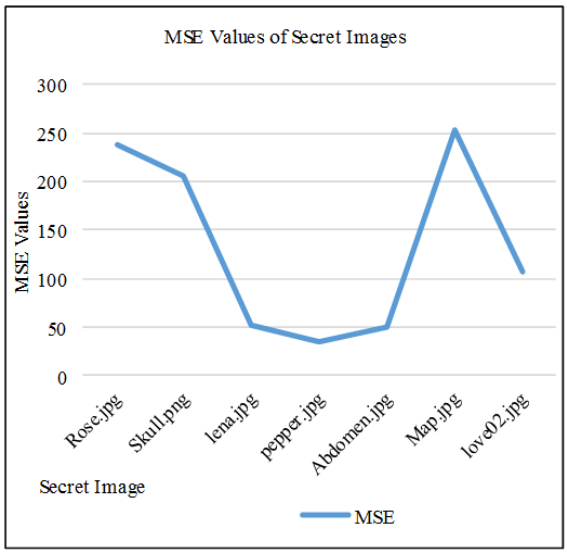

Fig.9. MSE values of Original and Extracted Secret Image from Urscent.avi

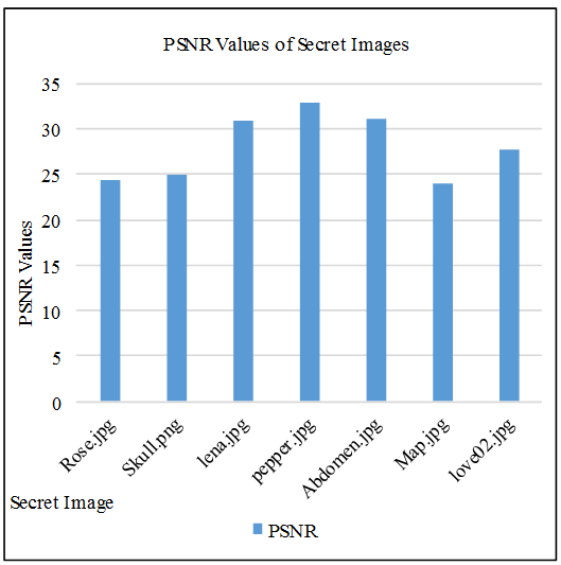

Fig.10. PSNR values of Original and Extracted Secret Image from Urscent.avi

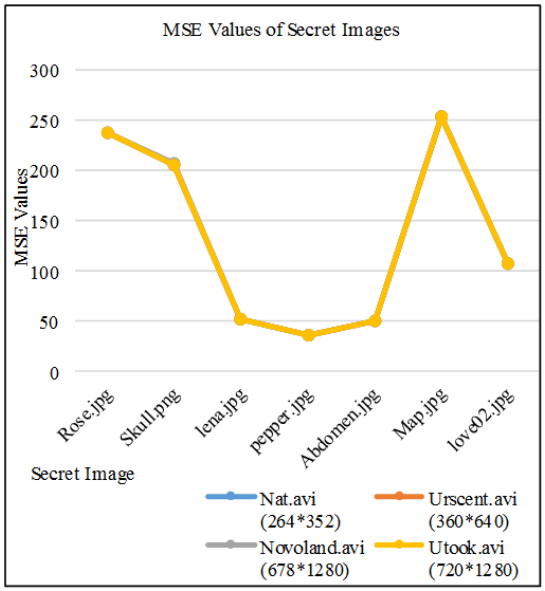

Fig.11. MSE results for original secret images and extracted secret images of different video quality files

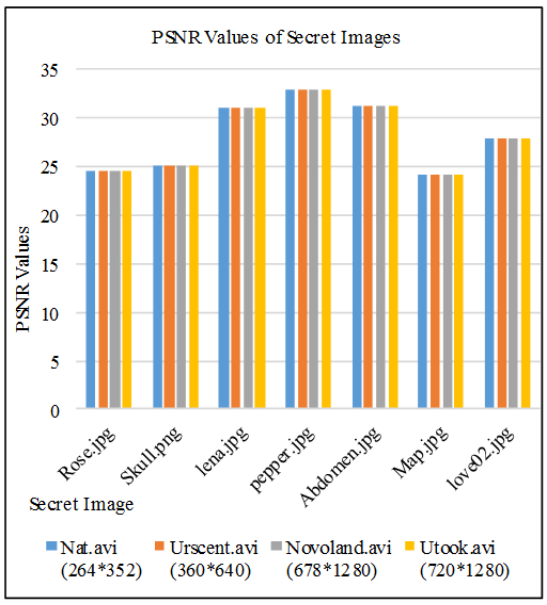

Fig.12. PSNR results for original secret images and extracted secret images of different video quality files

As the another experiment of the system, it is tested by slat & pepper noise attack with different noise density (0.01, 0.03, 0.05, 0.08). Fig. 13 shows the original secret image (pepper.jpg (512*512)) and fig. 14, fig. 15, fig. 16 and fig. 17 are the extracted secret images from the stego video file that is attacked by different noise density. Beside then, these test was done over different secret image such as lena.jpg and Abdomen.jpg with different noise density. In this test, the secret image Lena.jpg is embedded in a video file and the stego video file is also attacked by salt & pepper noise with different noise density (0.01, 0.03, 0.05 and 0.08). Then, the secret image is extracted from each attacked stego file and evaluated PSNR ratio of original secret image and extracted secret image. Results are itemized in fig. 18. As this way the other secret images Pepper.jpg and Abdomen.jpg are also tested and evaluated their PSNR ratios over each noise density, it is shown in fig. 19 and fig. 20. Moreover, the available PSNR and MSE results of this noise test are detail expressed in table 1.

Fig.13. Original secret image (Pepper.jpg)

Fig.14. Extracted secret image (Pepper.jpg)after salt & pepper(0.01) noise attack

Fig.15. Extracted secret image (Pepper.jpg) after salt & pepper (0.03) noise attack

Fig.16. Extracted secret image (Pepper.jpg) after salt & pepper (0.05) noise attack

Fig.17. Extracted secret image (Pepper.jpg) after salt & pepper (0.08) noise attack

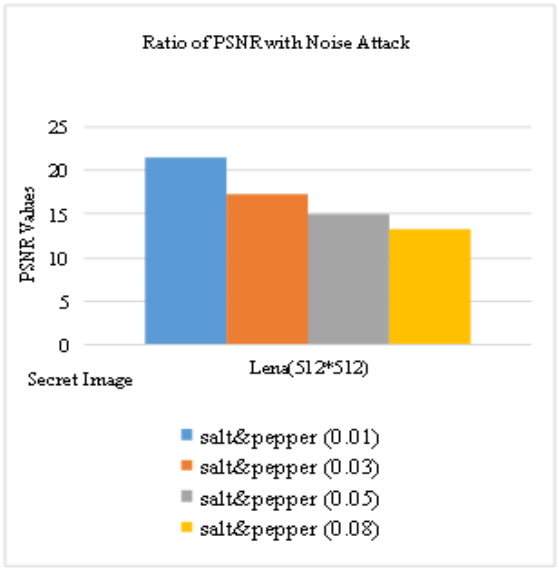

Fig.18. PSNR ratio of extracted secret image (Lena.jpg) with different noise density attack

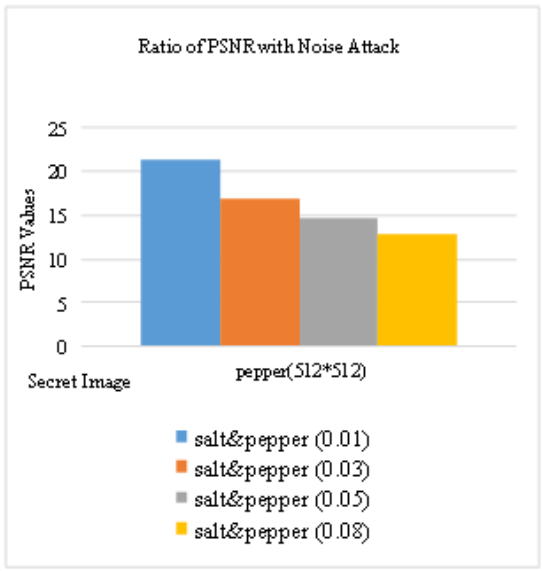

Fig.19. PSNR ratio of extracted secret image (Pepper.jpg) with different noise density attack

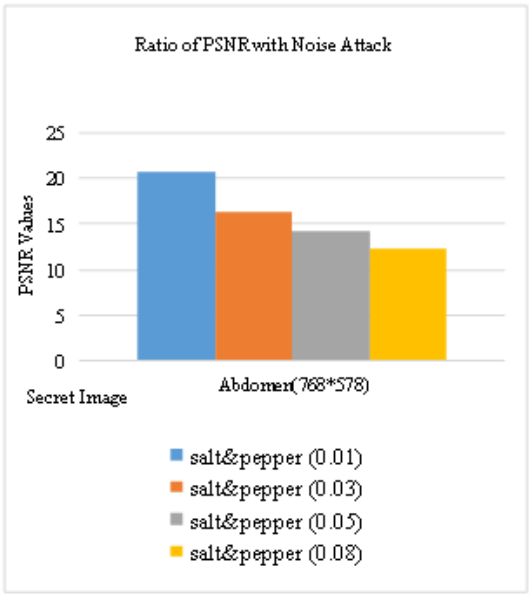

Fig.20. PSNR ratio of extracted secret image (Abdomen.jpg) with different noise density attack

V. Conclusions

The system provides enhanced security to the secret message by combination of steganography and cryptography. As a preprocessing stage, to support secure system transformation and scrambling methods are used so, it also found that a minimum distortion made to the extracted secret image. Then to provide higher level security, double key encryption technique is also used. Information security using data hiding in Audio-Video provide better hiding capacity and security. The main features of this system are imperceptibility, security,

robustness and to use real time image. Thus, for hiding secret information and achieving secrecy, this system is strong and secure. Therefore, the combination of steganography and cryptography system supports that the convert communication between sender and receiver can be effective.

Table 1. Results of MSE and PSNR with Noise Attack

Image (Size)	Noise Attack (salt & pepper)							
	Noise density = 0.01		0.03		0.05		0.08	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena.jpg (512*512)	469.5221	21.4558	1.2715e+003	17.1470	2.0805e+003	14.9998	3.1263e+003	13.2387
Pepper.jpg (512*512)	473.1420	21.3996	1.3576e+003	16.8133	2.1843e+003	14.7495	3.3976e+003	12.8307
Abdomen.jpg (768*578)	559.4072	20.6614	1.5502e+003	16.2354	2.5034e+003	14.1531	3.8586e+003	12.2736

REFERENCES

[1] 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

[2] Praveen. P and Arun. R, "Audio-Video Crypto Steganography Using LSB substitution and advanced chaotic algorithm", International Journal of Engineering Inventions, e-ISSN: 2278-7461, p-ISSN: 2319-6491, Volume 4, Issue 2 (August 2014)

[3] Sadik Sli AI-Taweel, M. Husain AI-Hada and Ahmed Mahmoud Nasser, "Image in image Steganography Technique based on Arnold Transform and LSB Algorithms", International Journal of Computer Applications (0975-8887), Volume 181- No.10, August 2018

[4] Sghaier Guizani and Nidal Nasser, " An Audio/Video Crypto- Adaptive Optical Steganography Technique", 978-1-4577-1379-8/12/$26.00c2012 IEEE

[5] Prof. D.J.Bonde and et al, " Application of Data hiding using Anti-Forensic Technique", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, p- 2395-0072, Volume:03, Issue:03,Mar-2016

[6] Rambabu Mudusu, A. Nagesh, M. Sdanandam," Enhancing Data Security Using Audio-Video Steganography", International Journal of Engineering & Technology. 7(2.20) (2018) 276-279

[7] 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.

[8] 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

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

[10] Majid Bakhtiari and Mohd Aizaini Maarof, "An Efficient Stream Cipher Algorithm for Data Encryption", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No.1, May 2011, ISSN (Online): 1694-0814.

[11] Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol.3, Issue 1, January-February 2013, pp.1641-1644

[12] Anita Pradhan and et al, 'Performance Evaluation Parameters of Image Steganography Techniques', International Conference on Research Advances in Integrated Navigation System (RAINS-2016), April 06-07, R. I. Jalappa Institute of Technology, Doddaballapur, banglore, India.

[13] Abhinav Thakur, Harbinder Singh and Shikha Sharda, ' Secure Video Steganography based on Discrete Wavelet Transform and Arnold Transform', International Journal of Computer Application (0975-8887), Volume 123-No.11, August 2015

[14] Madhuri R. Shende, Prof. Amit Welkar and Prof. S.V. Wajurkar Nagpur, 'Advanced Steganography for Hiding Data and Image using Audio-Video', International Conference on Modern Trends in Engineering Science and Technology (ICMITST 2016), Volume 2, Issue 5, ISSN 2454-4248, 24-30

[15] Olatunde Yusuf Owolabi, P.B. Shols and Muhammed Besiru Jibrin, ' Improved Data Security System Using Hybrid Cryptosystem', 2017 IJSRSET, Volume 3, Issue 3, Print ISSN: 2395-1990, Online ISSN 2394-4099

[16] Daniyal M. Alghazzawi, Syed Hamid Hasan and Mohamed Salim Trigui,' Stream Ciphers: A Comparative Study of Attacks and Structures', International Journal of Computer Applications (0975-8887), Volume 83-No1, December 2013

[17] Tarik Idbeaa, Salina Abdul Samad and Hafizah Husain, 'A Secure and Robust Compressed Domain Video Steganography for Intra- and Inter- Frames Using Embedded –Based Byte Differencing (EBBD) Scheme', PLoS ONE 11(3):e0150732. Doi:10.1371/ journal.pone.0150732, March 10, 2016

Authors' Profiles

Hnin Lai Nyo: born in 1988. Ph.D candidate in University of Technology (Yatanarpon Cyber City) from Pyin Oo Lwin, Myanmar.

She is an assistant lecturer in Computer University (Taungoo), Bago Region of Myanmar. In recent year, she was interested in the research field of Distributed System, image Processing and Information Security.

Aye Wai Oo: born in 1980. Professor and Ph.D supervisor in University of Technology (Yatanarpon Cyber City) from Pyin Oo Lwin, Myanmar. Her main research interests include Data Communication, Embedded System, Security, Image Processing.

How to cite this paper: Hnin Lai Nyo, Aye Wai Oo, "Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.6, pp.45-53, 2019.DOI: 10.5815/ijcnis.2019.06.06