

# Streaming Video Service Model using Secure Steganographic Method

Yunjung Lee

*Dept. of Computer Science and Statistics, Jeju National University  
rheeyj@jejunu.ac.kr*

## **Abstract**

*In this work, we propose new streaming video service model using steganographic data-hiding algorithm has been presented in the paper, in which it is fit for streaming video data to hide information related in copyright and authentication of video data. Secret information is encrypted by session key generated with symmetric key by pseudo-random number; shared by sender and receiver, that increases confidentiality. To share the secret key with video streaming server and customer, the server encrypts the secret key with customer's public key and sends it to customer. In the future work, we plan to optimize adaptive threshold and appropriate a period of time  $T$ , so that those are fit for streaming video service user's propensity.*

**Keywords:** *Steganography, Video Streaming, Data Hiding*

## **1. Introduction**

With The spread of wireless portable devices, people want to get digital video streaming services under ubiquities environment, that is, anywhere and anytime. Therefore many video and movie service providers, such as movie studios, Netflix, Amazon and Hulu, plan to convert the wired and download service of video into the wireless and streaming service of it. This type of service can be applied to many kinds of applications such as VOD TV and video conference as well as industrial, military or medical field. The privacy and security of digital videos service has become increasingly more important in computerized and connected world. Digital multimedia contents such as movie, video and music etc. must be protected in their copyright. There can illegal access or streaming that threats the copyright of the media data. Many researches seek to protect the private multimedia data that are exchanged over the wired and wireless networks.

Steganography is the technology that hides secret or private data into a carrier in invisible manner and has no one else except communicating entities perceive existing of secret data in there. While it uses cover data as a carrier for hiding secret information, there are varies study that uses image or video, as well as text file, audio file as cover data file. It is called stego data that secret data is inserted into cover data. In video streaming, video data file is used as a cover data. Since needs for video streaming service with security are increasing, more robust and secure service model of it is required. In this paper, we show that our model allows for new type of digital video streaming steganographic service where it can be more robust against analysis attack for location of hidden data.

The rest of this paper is organized as follows. In the next section we review existing researches related to steganography that are not addressed with the conventional cryptography. Section 3 provides our proposed service model for video streaming using

steganographic method. In Section 4, its experimental result and performance analysis is given. Finally, Section 5 holds our conclusions and suggestions for further research.

## 2. Related Works

Steganography is hiding hidden message in communication, and cover data are the carrier media of hidden message. Digital watermarking provides copyright protection for digital data, and it is method to embed perceptible or imperceptible messages into multimedia data for asserting the ownership [7]. Cover data and secret message can be any multimedia data such as text, audio, image and video. There are many data embedding researches in steganography or digital watermarking in text field [1, 2], audio field [3-5], image field [6-9] and video field [10-13].

Video is a sequence of still images. Steganographic data embedding in video is very similar to images. However, there are many differences between data hiding in images and video. One of the important differences is the size of the carrier media. Since video contain higher capacity than a still image, more secret messages can be embedded in the video file. Data hiding operations are executed entirely in the compressed domain [1]. The more amounts of data are embedded in the video sequences; the more constraints are there. Furthermore, steganographic data embedding on the streaming video demands real-time processing.

There are various systems for embedding secret data in visual media. There are two domains that differentiate steganographic methods, where the modifications are applied. In image and video media, the frequency domain is applied. There are many researches and applications to hide hidden data in images. But video streaming has received less attention in this respect. In [14], the authors proposed the use of steganography in MPEG files to send resynchronization signals. [15] presented scheme that embeds data in P- and B- frames [11].

Images and video steganographic techniques are classified into spatial domain and frequency domain. Embedding techniques in spatial domain are LSB and matrix embedding, and so on. Two important parameters for evaluating the performance of a steganographic system are capacity and imperceptibility. Capacity refers to the volume of data that can be hidden in the carrier media so that no perceptible change is introduced. Imperceptibility or transparency represents the invisibility of the hidden data in the cover media without degrading quality by data hiding [17]. There are two main classes in video steganography. One is to embed data into uncompressed video, which then is compressed [18, 19]. The other is to embed data in compressed video stream. The former issues how to make the embedded message against video compression. In the latter, since the video basically exists in the format of compression, it is more meaningful.

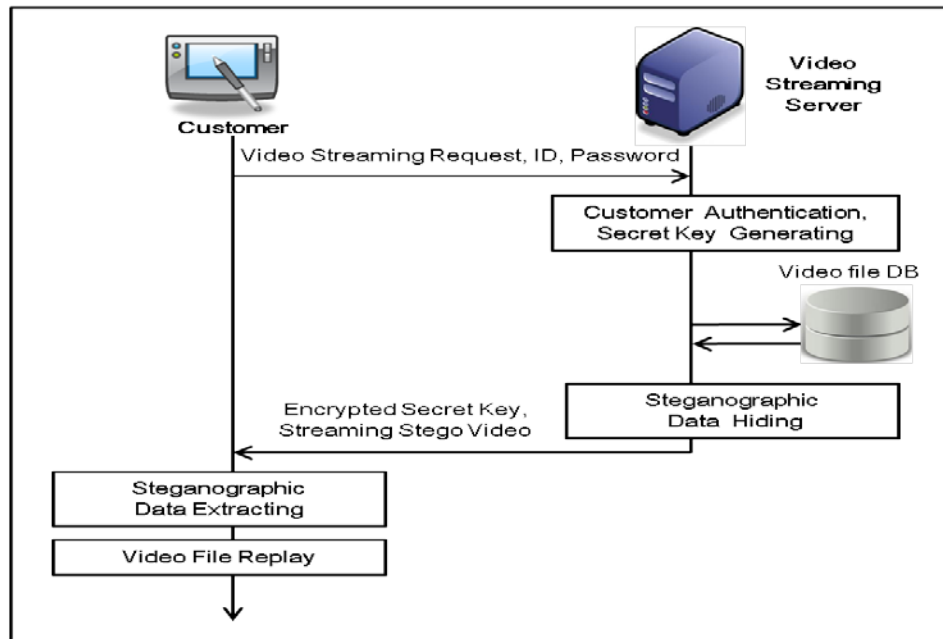
The goal of this work is to present the Steganographic Service Model for Streaming Video that can provide robust security with high computing speed in order to embed secret data into video file without perceptible changes.

## 3. Proposed Model and Algorithm

### 3.1. Service Model Structure

Y. Lee, B. Lee and C. S. Kim [5] presented audio streaming service model and algorithm for steganographic processing. It is suitable for feature of streaming audio book service in order to hide information of copyright and authentication of it. Secret information is encrypted with session key by secret key that client and server share, in order to improve confidentiality. It made secret data distributed randomly and evenly within cover data, and

improved throughput by simplifying additional computations considering streaming environment. We modify [5] and make it fit for video streaming environment. The proposed service model is given in Figure 1.



**Figure 1. Video Streaming Steganographic Service Model**

1. Customer requests video streaming service through wired or wireless communication like Internet, Wi-Fi or cellular channel to the server of video streaming service provider.

2. The server authenticates the customer, and creates session key used in transmitting stego video data. Then, it sends encrypted session key with customer's public key and retrieves appropriate video file from the video file database, and embeds secret messages like copyright or ownership information into cover media, video file, by steganographic manner. After that, it sends the stego video file where secret messages are inserted.

3. While stego video file is received, the customer, if needs, extracts hidden messages from stego video file received and replays transmitted the video file (stego video file).

The next section presents LSB inserting method for secure and faster steganographic data embedding and extracting in streaming situation.

### 3.2. Secret Key Generating and Sharing

Customer sends request of video file what he/she wants and data for authentication like ID and Password to video streaming server. Then the server authenticates the customer and generates secret key,  $K$ , used as a session key, and encrypts it with Customer's public key,  $K_{cs-pu}$ , and send it,  $K' (=E\{K\}_{K_{cs-pu}})$ , to the customer. The Customer receives  $K'$ , and decrypts  $K'$  with his/her private key,  $K_{cs-pr}$ , and get the secret key,  $K (=D\{K'\}_{K_{cs-pr}})$ .

$$K' = E\{K\}_{K_{cs-pu}} \quad (1)$$

$$K = D\{K'\}_{K_{cs-pr}} \quad (2)$$

### 3.3. Secret Messages Embedding and Extracting

After retrieving appropriate file from video file DB, video streaming server embeds hidden messages encrypted with session key, K, into cover video. Receiver can extract and get the hidden messages through reverse processing against embedding processing. Figure 2 shows the general embedding and extraction processing.

Pseudo-random number generator (PRNG) generates a session key S-K, using secret key K shared with sender and receiver as a seed value. Secret messages X are encrypted to X' on sender side and X' are decrypted from X on receiver side, by Block Cipher algorithm with the session key S-K in order to improve the security of secret messages. Therefore, anyone who tries to do illegal access into the hidden messages can be blocked even if he or she gets the algorithm used.

$$S-K = PRNG(K) \tag{3}$$

$$X_i' = E(X_i)_{S-K} \tag{4}$$

$$X_i = D(X_i')_{S-K} \tag{5}$$

where, S-K : Session Key; PRNG : Pseudo-Random Number Generator;  $X = \{X_1, X_2, \dots, X_n\}$ ;  $X' = \{X_1', X_2', \dots, X_n'\}$

A video stream consists of collection of frames and the secret messages are inserted in these frames. The cover video is broken down into frames. The proposed scheme adopts [16], in which embeds eight bits of secret messages at one time in Least Significant Bit (LSB) of Red, Green and Blue (RGB) pixel of the cover video frames in 3 bits, 3 bits and 2 bits order respectively. The bit pattern for distributing messages is from the reason why the chromatic impact of blue to awareness of human eye is more serious than red and green. The scheme is shown in Figure 3.

Most of video file get pretty more file size and playing time than any other kinds of file, and it is unpredictable when user on streaming service quits the streaming. Therefore, secret messages have to be embedded within a period of time T, which most of user (receiver) might receive and plays for. In the next work, it has to be researched to optimize adaptive threshold and appropriate a period of time T, so that those are fit for streaming video service user's propensity.

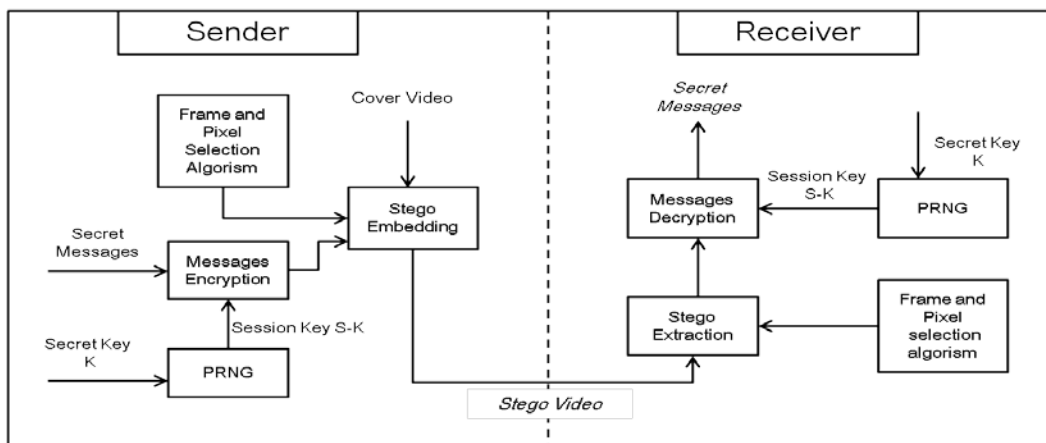
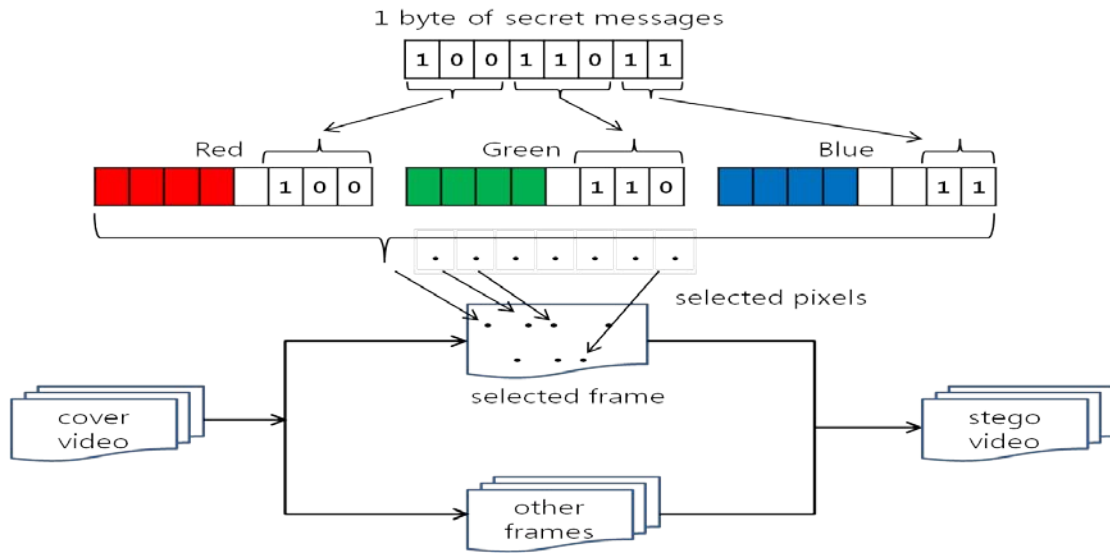


Figure 2. Steganographic Embedding and Extraction



**Figure 3. Frames and Pixels Selection**

#### 4. Experimental Results

Steganography scheme is evaluated by imperceptibility and capacity. Imperceptibility is measurement whether the embedded data is imperceptible to the human eye and statistical analysis or not. To demonstrate the performance of the proposed scheme, we evaluate a video streams (train.avi) and one secret data (jeju-logo.png). The imperceptibility of the embedded message is indicated by comparing the original video to its stego video to measure the visual change between them. Add to this, Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) is determined. PSNR is used to evaluate the invisibility of the stego frames. MSE is the simplest and full reference quality measurement, computed by averaging the squared intensity differences of changed and reference image pixels, along with the related quantity of PSNR [15, 16].

The details of cover file video and secret message are shown in Table 1 and the results are in Table 2. In Figure 4, we show several sample frames out of cover video (train.avi) and its stego.

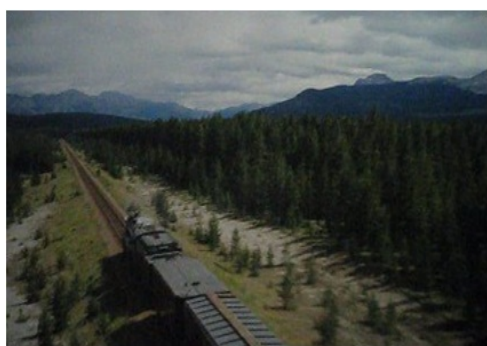
And the last, the histograms of before-frame and after-frame of message hiding are shown in Figure 5. Histogram is an important digital image tool of the distribution of data. It is an estimate of the probability distribution of a continuous variable. It represents tabulated frequencies and that especially in image, how many pixels are there with each value.

**Table 1. Cover Video and Secret Message Details**

Cover Video (train.avi)			Secret Message (jeju-logo.png)
Resolution	Frame/sec	No. of frames	Resolution
256 * 240	30	180	276 * 372

**Table 2. Results from PSNR and MSE**

Frame No.	PSNR	MSE
frame 1	46.3	0.34
frame 2	42.7	0.37
frame 3	44.2	0.35



Frame 1 (a)



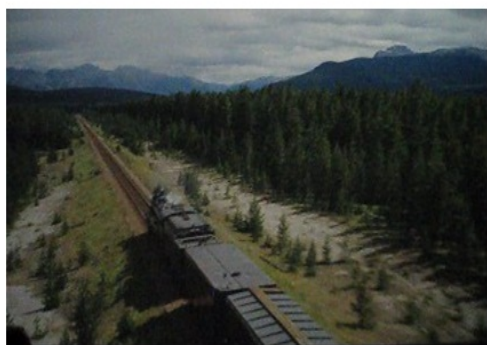
Frame 1 (b)



Frame 2 (a)



Frame 2 (b)

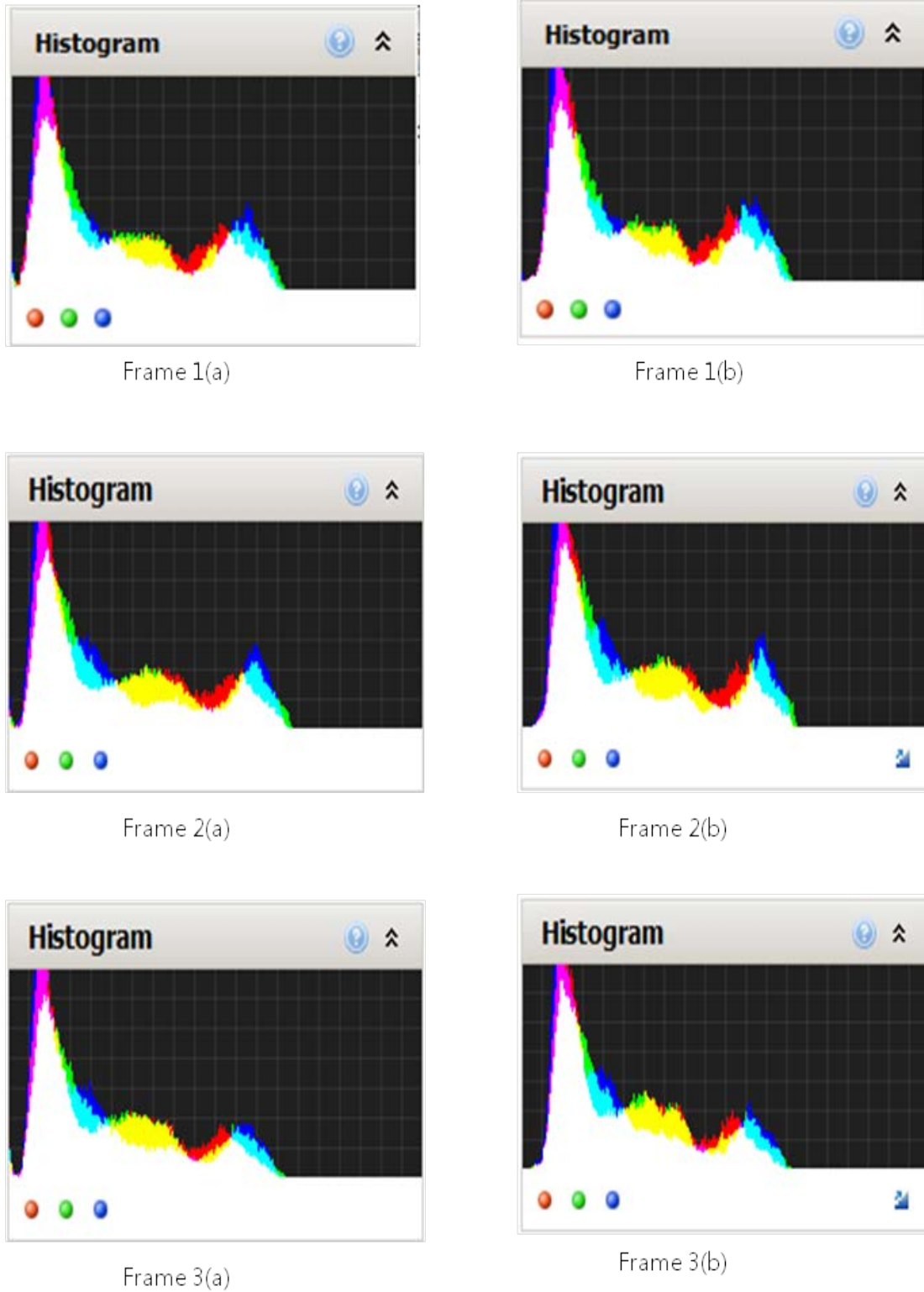


Frame 3 (a)



Frame 3 (b)

**Figure 4. Frame 1(a), 2(a), 3(a) : Cover Frames; Frame 1(b), 2(b), 3(b) : Stego Frames**



**Figure 5. Histograms of Original Video Frames and Stego Video Frames**

## 5. Conclusion

New streaming video service model using steganographic data-hiding algorithm has been presented in the paper, in which it is fit for streaming video data to hide information related in copyright and authentication of video data. Secret information is encrypted by session key generated with symmetric key by pseudo-random number; shared by sender and receiver, that increases confidentiality. To share the secret key with video streaming server (sender) and customer (receiver), the server encrypts the secret key with customer's public key and sends it to customer. In the future work, we plan to optimize adaptive threshold and appropriate a period of time, so that those are fit for streaming video service user's propensity.

## Acknowledgements

This research was supported by the 2013 scientific promotion program funded by Jeju National University.

## References

- [1] D. Bhattacharyya, P. Das, S. Kumar Bandyopadhyay and Taihoon Kim, Text Steganography: A Novel Approach, International Journal of Advanced Science and Technology, Volume 3, pp.79-86, (2009) April 5-7
- [2] Mohit Garg, A Novel Text Steganography Technique Based on Html Documents, International Journal of Advanced Science and Technology (IJAST), Volume 35, pp.129-138 (2011)
- [3] N. Cvejic and T. Seppanen, Increasing Robustness of LSB Audio Steganography using a Novel Embedding Method. Proceedings of the IEEE International Conference of Information and Tech : Coding and Computing, (2004) April 5-7
- [4] S.S. Agaian, D. Akopian, O. Caglayan and S. A. D'Souza, Lossless Adaptive Digital Audio Steganography. Proceedings of IEEE International Conference of Signals, Systems and Computers, (2005) October 28 - November 1
- [5] Y. Lee, B. Lee and C. S. Kim, Secure Steganographic Model for Audio e-Book Streaming Service, Journal of the Korea Academia-Industrial Cooperation Society, Vol.12, No.12, pp.5878-5884 (2011)
- [6] C. Hsieh, Y. Wu, and K. Hung, Hybrid Watermarking Scheme for Halftone Images, International Journal of Advanced Science and Technology, Volume 1, pp.9-20 (2008)
- [7] G.RoslineNesaKumari, B. VijayaKumar, L.Sumalatha, and Dr V.V.Krishna, Secure and Robust Digital Watermarking on Grey Level Images, International Journal of Advanced Science and Technology, Volume 11, pp.1-8 (2009)
- [8] M.M.Sathik and S.S.Sujatha, An Improved Invisible Watermarking Technique for Image Authentication, International Journal of Advanced Science and Technology, Volume 24, pp.61-74 (2010)
- [9] Ko-Chin Chang., Chien-Ping Chang., Ping S. Huang., and Te-Ming Tu, A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia, Volume 3, No. 2 (2008)
- [10] A. P. Sherly and P. P. Amritha, A Compressed Video Steganography using TPVD, International Journal of Database Management Systems, Volume.2, No.3 (2010)
- [11] D. Stanescu, M. Stratulat, B. Ciubotaru, D. Chiciudean, R. Cioarga and M. Micea, Embedding Data in Video Stream using Steganography. Proceeding of International Symposium on Applied Computational Intelligence and Informatics, (2007) May 17-18
- [12] A. Westfeld and G. Wolf, Steganography in a Video Conferencing System, Information Hiding, Lecture Notes in Computer Science, Volume 1525 (1998)
- [13] D. Socek, H. Spyros, S. Magliveras, O. Marques, D. Culibrk and B. Furht, New approaches to encryption and steganography for digital videos, Multimedia Systems, Volume 13, Issue 3 (2007)
- [14] D. Robie and R. Mersereau, Video Error Correction using Steganography. Proceedings of International Conference on Image Processing, Volume 1, (2001) October 7-10
- [15] S.Fong and S.Y. Zhuang, P.B. Ray, and S. Singh, An Efficient Digital Watermarking Algorithm for MPEG Video. Proceedings of International Conference on Signal Processing, Pattern Recognition, and Applications, (2002); Crete, Greece
- [16] K. Dasgupta, J. K. Mandal and P. Dutta, Hash Based Least Significant Bit Technique for Video Steganography (HLSB), International Journal of Security, Privacy and Trust Management (IJSPTM), Volume 1, No. 2 (2012)

- [17] Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, Video Steganography using Motion Vector and Linear Block Codes. Proceedings of IEEE International Conference on Software Engineering and Service Sciences (ICSESS), (2010) April 5-7; Beijing, China
- [18] E. Cole and R.D. Krutz, Hiding in Plain Sight, Steganography and the Art of Covert Communication, Wiley Publishing, Inc., ISBN 0-471-44449-9, (2003)
- [19] Stefan Katzenbeisser and Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Books, ISBN 1-58053-035-4, (1999)

### Author



**Yunjung Lee**, did her Bachelor's and Master's in the Department of Computer Science from Sook-Myung University, Seoul, South Korea in 1998. Subsequently, she did her Ph.D. in the Department of Computer Science from Korea University, Seoul, South Korea in 2002. She's been a professor of the Department of Computer Science and Statistics in Jeju National University, Jeju, South Korea from 2004.

