MPEG Video Content protection based on Fingerprinting Scheme

Seunglim Yong[†]

Institute for Graphic interfaces, KOREA

Summary
The paper presents a system for the secure distribution of a copyrighted video based on fingerprinting scheme. A combined selective watermarking and encryption method that operates in the compressed MPEG domain is introduced. Watermarking resistant to a number of attacks is used for copyright protection. The video quality deteriorates significantly due to encryption, thus restraining unauthorized viewers from viewing it. The video can only be viewed using the developed Secure MPEG player, which performs real-time decryption of the encrypted video.

Key words:
Fingerprinting, MPEG Video, Encryption, Watermarking.

1. Introduction

The illegal copying and redistribution of digital content is a crucial problem to distributors who electronically sell digital content. Digital fingerprinting schemes are an important class of protection techniques of intellectual property. Fingerprinting schemes support the copyright protection by enabling the original content provider to identify a traitor who originally purchased the data item. Fingerprinting schemes can be classified into the following three classes: Symmetric, asymmetric and anonymous asymmetric. In symmetric schemes, the content provider fingerprints digital contents, slightly differently from the original data item and unique to the buyer, and distributes the digital data. Thus the malicious content provider himself could spread the version sold to some buyer and then accuse that buyer of his own actions[1,2, 11,12]. In asymmetric schemes, the buyer and the content provider perform interactive protocol where the buyer embeds his own secret to fingerprint the copy. At the end of the protocol only the buyer knows the fingerprinted copy. The advantage of this solution is that the content provider can obtain proof against the buyer that can convince any honest third party. But the drawback is that the content provider knows the buyer's identity even when the buyer is innocent[8]. In anonymous asymmetric fingerprinting, the buyer can purchase a fingerprinted copy without revealing his identity to the content provider. The buyer no longer has to identify himself when purchasing the copy and remains anonymous as long as he keeps the purchased good secret, i.e., does not distribute it. More precisely, the content provider can learn the buyer's identity only if he obtains the purchased copy. Upon finding a fingerprinted copy, the content provider needs the help of a registration authority to identify a traitor[4,5,7,8].

In this paper, we proposed an MPEG video content protection scheme based on fingerprinting protocol. The proposed method first watermarks the selected I-frame data and then encrypts them using the symmetric encryption algorithm. Based on commutative encryption scheme, key sequence, which are used to decrypt digital contents, is double locked by two encryption keys kept separately by the buyer and the key management center. Since the key management center does not know the key sequence chosen by the buyer, proposed scheme does not need the trusted third party for fair transaction and an anonymous property is achieved. In the protocol, the buyer only gets a few of keys and can decrypt a few of fingerprinted digital contents in a transaction and the content provider has no idea how the fingerprint is formed. This facilitates the authority to determine the unethical party in case of illegal distributions of digital contents.

2. Related works

2.1 Fingerprinting scheme

Fingerprinting schemes can be classified into the following; Symmetric, asymmetric and anonymous asymmetric. In symmetric schemes, the content provider fingerprints the digital data, slightly differently from that of the original data and unique to that of each buyer's copy. Consequently, a malicious content provider could sell digital data with the same fingerprint to numerous buyers and accuse a buyer of being the traitor[8]. In asymmetric schemes, the buyer and the content provider perform interactive protocol where the buyer embeds his own secret to fingerprint the copy. At the end of the protocol

Manuscript received October 5, 2007
Manuscript revised October 20, 2007

only the buyer knows the fingerprinted copy. The content provider can obtain proof against the buyer that can convince any honest third party. But the drawback is that the content provider knows the buyer's identity even when the buyer is innocent[12]. In anonymous asymmetric fingerprinting, the buyer can purchase a fingerprinted copy without revealing his identity to the content provider. The buyer no longer has to identify himself when purchasing the copy and remains anonymous as long as he keeps the purchased good secret. Upon finding a fingerprinted copy, the content provider needs the help of a registration authority to identify a traitor.

2.2 MPEG Compressed Video

MPEG is a lossy compression technique which retains only enough information for recovering the most significant parts of a compressed video stream [6]. In order to meet random access requirements without compromising quality requirements for high compression, MPEG introduced the concept of a “group of frames” in Fig. 1.

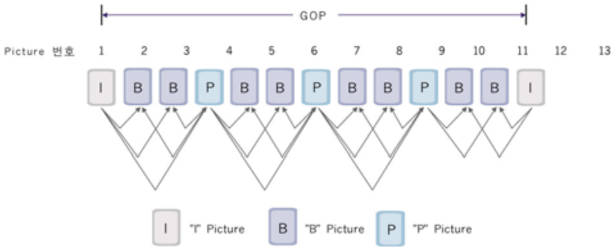
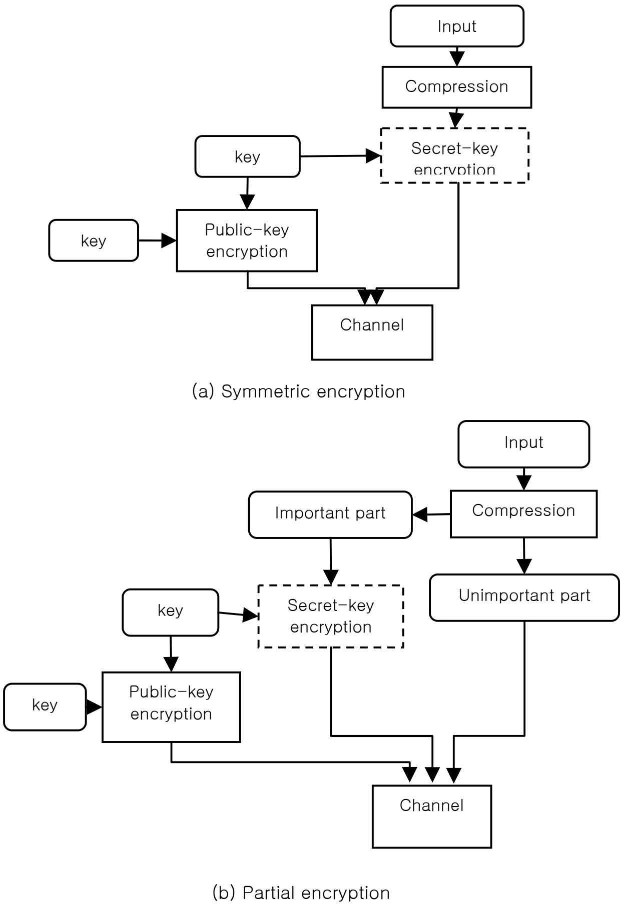


Fig. 1 MPEG frame architecture

This group of frames contains a well balanced combination of both intraframe (stand-alone) and inter-frame coded frames. The intraframe coded “I’ frames provide points for random access. High compression is maintained by use of predicted (“P”) and interpolated (“B”) interframe coded frames, which are based on adjacent “I” frames.

2.3 Partial Encryption

In order to prevent unauthorized viewing of the watermarked video stream, partial encryption is employed The proposed encryption scheme encrypts only the I-frames, as was hyphenation also proposed by other researchers [6,10], in order to save encryption and decryption time. Due to the MPEG coding structure, distorting the intra frames i.e., encrypting the I-frames, leads at the same time to reproducing distorted P and B-frames. However, the MPEG encoders sometimes produce P- or B-frame macroblocks that are intracoded. These macroblocks will not be encrypted, hence they will be correctly decoded even if the I-frame of the same group of pictures (GOPs) is encrypted. In such a case, the corresponding decoded macroblocks of the P- or B-frames will not be distorted, leading to video frames with visible parts even without carrying out decryption. Fig. 2 shows the difference between original symmetric encryption and partial encryption.



(a) Symmetric encryption

(b) Partial encryption

Fig. 2 Symmetric encryption and partial encryption

3. Overview of our scheme

The involved parties in our protocol and roles of each entity are as following.

- Buyer(*B*) : She has to register to *RC* to obtain her own anonymous public key. She delegates the power of signing and protocol execution to a mobile agent who will execute protocols instead of herself. She issues the proxy signature pair.

- Content provider(CP) : He is an agent selling digital contents. He has database to record anonymous buyers and their information. He has to embed the anonymous buyer's information into digital contents without revealing it.
- Registration Center(RC) : The buyer registers anonymous key pair to registration center.
- Judge(J) : We assume that judge is a trusted third party.

For the purpose of fingerprinting, it is required in this model that buyers register themselves to RC. There is no special restriction on J. The main subprotocols of the construction are registration, delegation, fingerprinting, and identification.

There are two steps where fingerprinting techniques are used for rightful ownerships. In the first step, the content provider inserts two fingerprints into the digital content and encrypts it with symmetric key cryptosystem. The content provider generates two identical copies of MPEG video stream. The content provider generates different fingerprinted video contents $item_0$ and $item_1$ by embedding two fingerprints into each "I" frame. And he randomly generates two secret key vectors K_0 and K_1. Then the content provider encrypts $item_0$ with key vector K_0 and $item_1$ with key vector K_1 using symmetric key cryptosystem. Each key vector consists of t different keys and each frame of $item_i$ is encrypted by each key of key vector K_i. In the second step, the content provider encrypts two secret key vectors using commutative encryption algorithm. The buyer obtains t keys, which enables him to decrypt the encrypted contents, by choosing, at his own will, the first key of the key vector from either K_0 or K_1, the second key of the key vector from either K_0 or K_1, and so on. After obtaining t keys, the buyer can decrypt the encrypted digital contents with the selected keys. Fig.3 shows the process of decryption

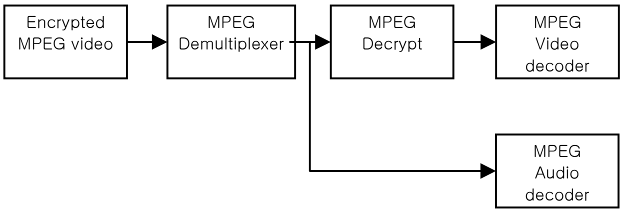


Fig. 3 MPEG frame architecture

A detailed description of the protocol will be given in section 4.

4. Fingerprinting protocol

In this section, we propose an efficient anonymous fingerprinting scheme for MPEG video.

Notation The fingerprinted copy, some of its bits can be altered, remains "close" to original copy. But without knowing which particular bits were changed, the altering of these bits is impossible without rendering the content useless. We refer to the formal definition of "marking assumption"[3]. We establish some notation as the following.

- + : Fingerprint embedding operation
- SE/SE^{-1} : Symmetric encryption/decryption algorithm
- CE/CE^{-1} : Commutative encryption/decryption algorithm
- E: Public key encryption algorithm
- H: Collision-free one-way hash function

4.1 Registration

Assume that both the buyer and the registration center have public and secret key pairs. The buyer's secret key is x_B and his public key is $y_B = g^{xB}$. The registration center uses its secret key to issue certificates which can be verified using the registration center's public key. The public keys of the registration center and all buyers are assumed to be known and certified.

1) $\boldsymbol{B}$ randomly chooses two secret values $x_1, x_2 \in Zp$ such that $x_1 + x_2 = x_B \in Zp$. $\boldsymbol{B}$ generates the signature $Sig(H(x_2))$ with x_1. $\boldsymbol{B}$ sends y_B , $y_1(y_1 = g^{x1}$), $E_{RC}(x_2)$ and $Sig(H(x_2))$. The buyer can convince the registration center by generating the signature $Sig(H(x_2))$.

2) RC decrypts $E_{RC}(x_2)$ and verifies the signature $Sig(H(x_2))$. If the signature is OK, RC computes $y_2 = g^{x2}$ and checks that $y_1y_2 = y_B$. If it is verified, it returns to $\boldsymbol{B}$ a certificate $Cert(y_1)$. The certificate states the correctness of y_1 and registration of $\boldsymbol{B}$.

4.2 Fingerprinting

We now describe the fingerprinting protocol between a buyer and a content provider. The protocol begins by generating fingerprinted contents.

Let *item* = {$item_j$|0 ≤ j ≤ t} be the I-frame of MPEG compressed video of the content provider. The fingerprinting protocol is performed as follows:

Step.1 Encrypt fingerprinted contents

1) Two kinds of packets $item^{0,j}$ and $item^{1,j}$ are calculated for one packet $item_j$ by embedding information bit “0” as a first fingerprint F_0 and “1” as a second fingerprint F_1, respectively.

2) *CP* generates two secret key vectors K_0 and K_1. Each key vector consists of *t* keys which are arbitrarily selected.

$$K_0 = \{k_{0,1}, k_{0,2}, ..., k_{0,t}\} \text{ , } K_1 = \{k_{1,1}, k_{1,2}, ..., k_{1,t}\}$$

3) Then *CP* encrypts the 2*t* frames of $item^i_B$ using 2*t* keys selected above. They are encrypted using symmetric key encryption(deterministic encryption algorithm, say, DES or AES). *CP* generates two encrypted digital content vectors X^0_B, X^1_B , and sends them to ***B***. The key vector K_i is used for encrypting $item^i_B$. That is .

$$X^i_B = SE(k_{0,j} \text{ , } itemi^{j}_B \text{)}$$

Encryption of the fingerprinted packets are shown in Figure 2.

4) The order of the two ciphertexts is rearranged by a permutation function $(X^0_{Bj,} X^1_B)$

Step.2 Encrypt key vectors

5) *CP* selects a secret key *S* and uses commutative encryption algorithm *CE* to encrypt the two key vectors $C_0 = \{c_{0,1}, c_{0,2}, ..., c_{0,t}\} = CE(S, k_{0,j})$ and $C_1 = \{c_{1,1}, c_{1,2}, ..., c_{1,t}\} = CE(S, k_{1,j})$ as shown in the following. Then *CP* sends C_0 and C_1 to ***B***.

6) When ***B*** receives C_0 and C_1, he constructs a new encrypted vector $C' = (c'_1, c'_2, ..., c'_t)$ by choosing c'_j from either $c_{0,j}$ or $c_{1,j}$. ***B*** generates a *t*-bit integer $L_B = H(x_2)$, which is denoted as a bit pattern $\{l_1, l_2, ..., l_t\}$. If the bit l_j = 0 then ***B*** chooses $c'_j = c_{0,j}$ and if the bit l_j = 1 then $c'_j = c_{1,j}$.

7) After generating *C’*, ***B*** randomly chooses a secret key *R* and uses *CE* to encrypt *C’* to get two encrypted vectors $D = \{d_1, d_2, ..., d_t\}$, where $d_i = CE(R, c'_i) = CE(R,CE(S, k_{lj,j})) = CE(S,CE(R, k_{lj,j}))$. Then ***B*** sends the encrypted vector *D* to *CP*.

8) ***CP*** decrypts vector *D* with *S* and gets the vector $U = \{u_1, u_2, ..., u_t\}$, where $u_i = CE^{-1}(S, d_i)$. After the decryption, ***CP*** sends *U* to ***B***.

9) ***B*** generates an encapsulated data $T_B = E_J(L_B)$ and a signature $Sig(T_B)$ and send them to ***CP***. The value T_B and $Sig(T_B)$ are used as evidence for solving possible piracy disputes in the future.

10) ***CP*** verifies the signature $Sig(T_B)$ with anonymous public key y_1. If it is OK , ***CP*** sends a signature of T_B to ***B***.

11) ***B*** now obtains decrypting keys by decrypting each u_i in vector *U* with the key *R* and can decrypt the encrypted digital content using K_B. *CP* keeps records Rec_B of all transactions in his database, where each transaction is summarized as a four-order tuple < $y_1,Cert(y_1), T_B, Sig(T_B)$ >.

When the buyer tries to decrypt a received ciphertext $(X^0_{B,} X^1_B)$, he obtains two bit strings. One is a properly packet that contains F_i, and the other is a random number that implies decryption failure. The buyer can obtain the fingerprinted content $item_B$. In our protocol, the merchant can embed a signal in his digital content; however, he cannot know which ciphertext of $(X^0_{B,} X^1_B)$ is decrypted by the buyer.

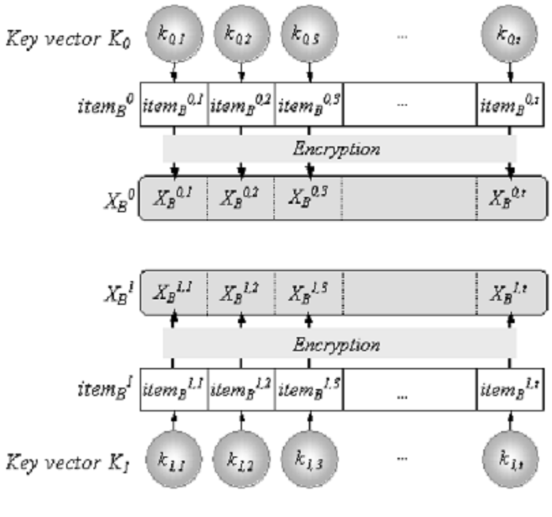


Fig. 4 Encrypt fingerprinted contents

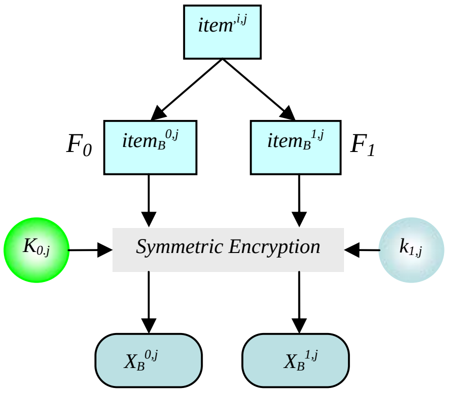


Fig. 5 Encrypt the packet

4.3 Tracing

After finding an illegally redistributed digital content, CP extracts the fingerprint pattern in it. If he succeeds, he sends the extracted fingerprint with the transaction record to ***J***, who will determine who is guilty by decrypting and checking the data T_B. ***J*** sends y_1 and asks for the value $H(x_2)$ to *RC* and verifies the fingerprint in the $item_B$ and checks the bit pattern whether L_B corresponds to the fingerprint pattern. And then ***J*** verifies the signature $Sig(T_B)$ with anonymous public key y_1 whether ***B*** generates T_B or not. If it is checked, asks for the identity of the traitor to *RC*. Thus *CP* can identify the traitor.

5. Security Analysis

In this section, we present the proof sketch in detail for the security of our protocol. We assume that all underlying primitives are secure, and the security of our scheme relies on that of the underlying watermarking algorithm and cryptosystem.

5.1 Security for the content provider

B wants to obtain two or more valid $item_B$ so that he can make unauthorized distributions of $item^0_B$ without being accused. However, ***B*** can only obtain one piece of valid fingerprinted content $item_B$ in the implementation of the protocol once. In our protocol, the digital contents are divided into *t* frames and each frame is encrypted by different keys. To acquire two or more valid $item_B$, ***B*** should obtain more than *t* keys in order to decrypt more than *t* frames of contents. But ***B*** can only obtain *t* keys. It is unlikely for *CP* to perform the decryption operation on more than one vector *D* sent by ***B***. Therefore, ***B*** cannot get two different key vectors by sending two *D* to *CP* and he can decrypt only *t* frames of encrypted digital content.

For redistributing the digital content without being accused, ***B*** is willing to make a false T_B by encapsulating a false L_B in the T_B sent to *CP*. In fingerprinting, ***B*** generates a *t*-bit integer L_B for choosing keys from vector C_0 and C_1, and finally obtains a corresponding fingerprinted content $item_B$.

Suppose ***B*** puts a false L'_B, instead of L_B, to generate $T'_B = E_J\,(L'_B)$, which is sent to *CP* to record. Although *CP* cannot notice ***B***'s trick, such cheating of ***B*** will be detected by *CP*. That is, when receiving an accusation request from *CP*, *J* verifies the signature $Sig(T_B)$. If it is verified, the fact is guaranteed that ***B*** generated the value T_B. ***J*** decrypts the T_B for checking. From the L'_B, ***B*** is judged to be guilty because the hash value of $H(x_2)$ from ***CP*** does not equal T_B Moreover, the signature $Sig(T_B)$ on T_B is used as non-repudiation evidence, so ***B*** cannot deny the fact that he has generated T_B.

So, we show that our protocol is secure against malicious buyer as well, which means that the buyer making unauthorized distribution will always be successfully identified.

5.2 Security for the buyer

We assume that ***RC*** does not reveal the buyer's ID if the buyer is honest. An honest buyer is secure if the attackers cannot convince the judge, even if the other parties collude and obtain other digital content that he bought. It is impossible for ***CP*** to figure out which information ***B*** selects, even if he is trying to make an incorrect performance. In fingerprinting, we can see that the only available information for ***CP*** from ***B*** is $D = \{d_1, d_2, ..., d_t\}$. To trace the origin of c_{0i}, in other words, to find out whether c_{0i} is c_0 or c_1, ***CP*** has to calculate c_{0i} from d_i without knowing *R*, which is the secret key held privately by ***B***. Such computation, however, is as hard to break as the encryption algorithm *CE*, which is generally agreed to be computationally intractable. Besides, the probability of *CP* knowing ***B*** chose whether c_{0i} is c_0 or c_1 on the total *t* frames would be equal to $1=2t$. Note that the value of *R* is randomly chosen by ***B*** in each transaction. There is no relation between the values of *R* and each of transaction.

Another possible attack from ***CP*** is to generate two pieces of identical fingerprinted contents instead of two different ones so that he can easily trace them. Such cheating of ***CP***, however, will be detected by ***J*** in our protocol. To cheat, ***CP*** generates the two identical copies of $item_i$ ***B*** with the same fingerprint. For example, ***CP*** generates two identical fingerprinted contents with the fingerprint pattern as {0, 1, 1, 0, ..1} and sends the encrypted forms to ***B***. In such case, ***B*** is not conscious of the cheating behavior of ***CP***, since $X^0{}_B$ and $X^1{}_B$ are not the same because each frame of $item^i_B$ is encrypted with different keys. But in fingerprinting, ***B*** arbitrarily chooses the bit pattern as {1, 0, 1, 1, ..., 0}, the bit pattern is different from the fingerprint pattern. That is, in identification protocol, since the bit pattern, which is generated by ***B***, and the fingerprint pattern are not in accord, ***J*** notices the cheating behavior of ***CP***.

6. Conclusion

In this paper, we have proposed an content protection scheme for MPEG video. We applied partial symmetric encryption algorithm for encrypting large amounts of MPEG video stream based on fingerprinting scheme. Through a security analysis, we have shown that our protocol is secure from both the content provider and the buyer. Since non-repudiation is also provided by the digital signature scheme, the buyer and the content provider cannot deny their actions. So the buyer cannot redistribute the purchased video.

References

[1] G. Blakley, C. Meadow and G. B. Purdy, “Fingerprinting long forgiving messages," Advances in Cryptology - CRYPTO'85, LNCS 218, pp. 180-189, 1986.

[2] D. Boneh and J. Shaw, “Collusion-secure fingerprinting for digital data," Advances in Cryptology - CRYPTO'95, LNCS 963, pp. 452-465, 1995.

[3] D. Chaum, “An impoved protocol for demonstrating possession of discrete logarithms and some generalizations," EUROCRYPT'87, LNCS 304, pp. 127-141, 1987.

[4] J. Domingo-Ferrer, “Anonymous fingerprinting based on committed oblivious transfer," PKC 1999, LNCS 1560, pp. 43-52, 1999.

[5] J. Domingo-Ferrer, “Anonymous fingerprinting of electronic information with automatic identification redistributors," IEE Electronic Letters, 43(13), pp. 1303-1304, 1998.

[6] Y. Li, Z. Chen, SM. Tan and RH. Campbell, "Security Enhanced MPEG Player," International Workshop on Multimedia Software Development(MMSD'96), pp. 169-175, 1996.

[7] B. Pfitzmann and A. R. Sadeghi, “Coin-based anonymous fingerprinting," Advances in Cryptology - EUROCRYPT'99, LNCS 1592, pp. 150-164, 1999.

[8] B. Pfitzmann and M. Schunter, “Asymmetric fingerprinting," Advances in Cryptology - EYROCRYPT'96, LNCS 1070, pp. 84-95, 1996.

[9] B. Pfitzmann and M. Waidner, “Anonymous fingerprinting," Advances in Cryptology - EUROCRYPT'97, LNCS 1233, pp. 88-102, 1997.

[10] G. Spanos and T. Maples, "Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications," IEEE International Phoenix Conference on Computers and Communications, pp. 72-78, 1996.

[11] W. Trappe, M.Wu and K. Liu, “Collusion-resistant fingerprinting for multimedia," IEEE International Conference on Acoustics, Speech, and Signal Processing, 4, pp. 3309-3312, 2002.

[12] N. R. Wanger, “Fingerprinting," IEEE Symposium on Security and Privacy, pp. 18-22, 1983.

Seunglim Yong received the B.S. and M.S. degrees in Computer Science and Engineering from Ewha Womans Univ. in 1998 and 2000, respectively. She received the Ph.D degrees in Computer Science and Engineering from Ewha Womans Univ. in 2006. During 2006-2007, he stayed in Ewha Womans Univ. as full time lecture. She now with Institute for Graphics Interface.