Journal of Korea Multimedia Society Vol. 12, No. 6, JUNE 2009(pp. 833-841)

Flexible Video Authentication based on Aggregate Signature

Weon Shin[†], Young-Jin Hong[††], Won-Young Lee[†††], Kyung-Hyune Rhee[††††]

ABSTRACT

In this paper we propose a flexible video authentication scheme based on aggregate signature, which provides authenticity of a digital video by means of cryptographic signature to guarantee right of users. In contrast to previous works, the proposed scheme provides flexible usages on content distribution system, and it allows addition of new contents to the signed contents and deletion of some parts of the signed contents. A modification can be done by content owner or others. Although contents are modified by one or more users, our scheme can guarantee each user's right by aggregation of the each user's signatures. Moreover, proposed scheme has half size of Digital Signature Algorithm (DSA) with comparable security.

Key words: Video Authentication, User Created Content, Content Recreation

1. INTRODUCTION

The use of digital video content instead of analogue data offers many advantages. It is possible to make an exactly same copy and edit it easily. Simultaneous, these advantages result in problems. Because, Anybody can edit and manipulate digital video content without special knowledges and distribute it through the World Wide Web. One solution for preventing illegal modification and preserving rights is digital video authentication.

Digital video authentication is a process that is used to ascertain the integrity of a digital video. And digital video authentication system should be able to determine whether the video has been tampered or not. To provide authenticity of digital video contents and owner's rights, digital video authentication is essential to prevent a video content from illegitimate users.

Conventional digital video authentication schemes are can be categorize into two parts. The first scheme is digital signature-based video authentication[1-3] that uses a conventional cryptographic signature scheme directly. In this scheme, the input is the hash value of the video data and is signed as general data. Its security is belongs to used cryptographic signature scheme. The second scheme is media signature-based video authentication[1,2]. It is similar to digital signature-based video authentication, while the difference between digital signature-based video authentication and media signature-based video authentication is the input data. The input of the second scheme is an extracted feature from video data or a hash value of the feature.

※ Corresponding Author : Kyung-Hyune Rhee, Address : (608-737) Daeyeon 3-dong, Nam-gu, Busan, Korea, TEL : +82-51-626-4887, FAX : +82-51-626-4887, E-mail : khrhee@pknu.ac.kr

Receipt date : Nov. 5, 2008, Approval date : Jan. 12, 2009

[†] Department of Information Security, Tongmyong University (E-mail : shinweon@tu.ac.kr)

[††] Department of Electrical & Electronic Engineering, Tongmyong University (E-mail : gryjhong@tu.ac.kr)

[†††] Department of Information Security, Pukyong National University (E-mail : gwangchi@pknu.ac.kr)

[††††] Division of Electronic, Computer and Telecommunications Engineering, Pukyong National University

※ This work was supported by the SKTU Institute of Next Generation Wireless Communications funded by SK telecom (SKTU-07-002)

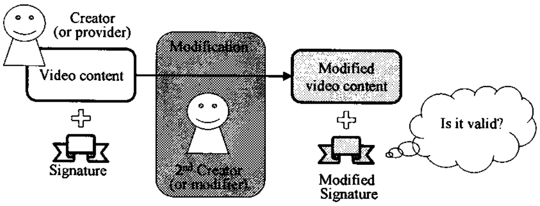


Fig. 1. Verification problem of modified video contents.

Conventional video authentication schemes do not allow any modification or allow only incidental distortion[1]. Some applications require modification of video contents for a flexible usage of contents. Fig. 1 shows that verification problem of modified video contents. In the distribution of video contents, if one user desires to modify partial data of a signed video content and make it possible to verify. The user discards prior authentication information to modify the video. And then, he/she extracts authentication information again from video content which is included in modified video data. But it is not a desirable way. Generally, the video contents tend to have huge amounts of data, and also the computational cost for extracting authentication information from them is high. Moreover it cannot guarantee prior user's right too.

In this paper we propose a new video authentication scheme. The proposed scheme provides authenticity of a digital video by use of cryptographic signature scheme and allows modification of video content by means of aggregation for the flexibility. Although modification is done by one or more users, our scheme can protect all the collaborated user's rights.

In Section 2 we present preliminaries of our scheme. In Sections 3 we describe the proposed scheme, a flexible video authentication based on aggregate signature derived from bilinear maps. Finally concluding remarks are given in Section 6.

2. PRELIMINARIES

2.1 Network Abstraction Layer Unit

H.264/AVC[4-6], which is developed as an extension earlier MPEG video coding standards such as MPEG-2(also known as ITU-T H.262) and H.263, is newest video coding standard of the ITU-T Video Coding Experts Group and the ISO/IEC Moving Picture Experts Group. The standard provides much higher compression efficiency and scalability functionalities than earlier standards. And also provides network-friendly video representation.

One characteristic feature of H.264/AVC is network abstraction layer (NAL). The coded video stream is organized into series of NAL units which contain an integer number of bytes to transmit the video packets effectively. The first byte of each NAL unit is a NAL header that indicates a type of NAL unit. The NAL header consists of one forbidden bit, nal_ref_idc and nal_unit_type. The remaining bytes contain variable length raw byte sequence payload (RSPB) of the type indicated by the header. Coded video data are stored in the RSPB.

The NAL unit structure specifies a generic format for use in both bitstream-oriented and packet-oriented transport systems, and series of NAL units generated by an encoder are referred to as NAL unit streams. In the bitstream-oriented format, each NAL unit is prefixed by a specific pattern of three bytes called a start code prefix. The boundaries of the NAL unit can be identified by searching the coded data for the unique start code prefix pattern. The use of emulation prevention bytes guarantees that start code prefixes are unique identifiers of the start of a new NAL unit. In packet-oriented format, the coded data is carried in packets that are framed by the system transport protocol, and identification of the boundaries of NAL units within the packets can be established without use of start code prefix patterns. In such systems, the inclusion of start code prefixes in the data would be a waste of data carrying capacity, so the replaced the NAL units can be carried in data packets without start code prefixes.

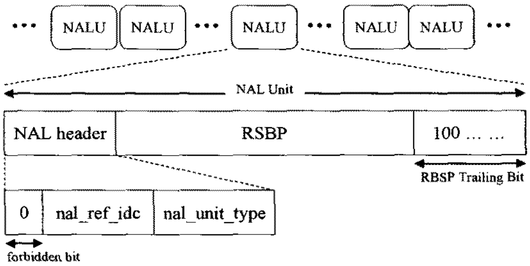


Fig. 2. NAL unit format

A set of NAL units in a specified form is referred to as an access unit. The decoding of each access unit results in one decoded picture.

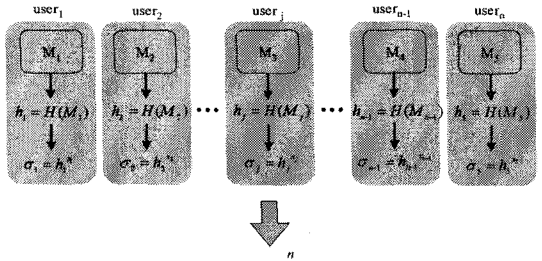
2.2 Aggregate Signature

In aggregate signature scheme[7-8], individual signatures are generated as similar as short signature[9] from individual messages by each users. The individual signatures are combined into an aggregate signature by using the aggregation algorithm. One or more users are can participate in the aggregation. And they need not be trusted each other, so they need not the redundant information for the aggregation. Fig. 3 shows the aggregate signature.

Throughout the paper we use the following notations:

- G is multiplicative cyclic groups of prime order p.
- g is a generator of G.
- e is bilinear map.
- H is cryptographic hash function.

and a bilinear map is a map $e: G \times G \rightarrow G_T$ -



$$\sigma = \sigma_1 \cdot \cdots \cdot \sigma_n = \prod_{i=1}^{n} \sigma_i \quad (1 \le i \le n)$$

Fig. 3. Aggregate signature.

where G_T is another multiplicative cyclic group of prime order p - with the following properties:

- Computable : there exists an efficiently - computable algorithm for compting $e(u,v)$, for all $u,v \in G$.
- Bilinear : for all $u,v \in G$ and $a,b \in Z, e(u^a,v^b) = e(u,v)^{ab}$.
- Non-degenerate : $e(g,g) \neq 1$.

The aggregate scheme includes the three usual algorithms for generating and verifying individual signatures, as well as two additional algorithms that provide the aggregation capability.

Key Generation. For a user, pick random $x \xleftarrow{R} Z_p$ and compute $v \xleftarrow{R} g^x$. The user's public key is $v \in G$. The user's private key is $x \in Z_p$.

Signing. Given the private key x and a message $M \in \{0,1\}^*$, compute $h \leftarrow H(v,M)$, where $H \in G$, and $\sigma \leftarrow h^x$. The signature is $\sigma \in G$.

Verification. Given a user's public key v, a message M, and a signature σ, compute $h \leftarrow H(v,M)$ accept the validity of signature σ if $e(\sigma,g) = e(h,v)$.

Aggregation. Arbitrarily assign to each user whose signature will be aggregated an index i, renging from 1 to n. Each user i provides a signature $\sigma_i \in G$ on a message $M_i \in \{0,1\}^*$ of her choice. Compute $\sigma \leftarrow \prod_{i=1}^{n} \sigma_i$. The aggregate signature is $\sigma \in G$.

Aggregate Verification. Given an aggregate signature $\sigma \in G$ for a set of users, indexed as before, and are given the original messages $M_i \in \{0,1\}^*$ and public keys $v_i \in G$. To verifiy the aggregate signature σ, compute $h_i \leftarrow H(v,M)$ for $1 \le i \le n$, and accept if $e(\sigma,g) = \prod_{i=1}^{n} e(h_i,v_i)$ holds.

Generated aggregate signature has the same length as a short signature. It means that the size of aggregate signature is half the size of DSA(Digital Signature Algorithm)[10] with comparable security[9]. So, the communicational cost is half compared with conventional digital signature. And the aggregate signature scheme is secure against existential forgery in the aggregate chosen-key model[9].

The aggregate signature has special characteristic that is possible adding a signatures into aggregated signature and removing individual signature from aggregated signature simply. In the Fig. 3, if there is a $user_{i+1}$ and he desires to aggregate his signature into aggregate signature σ, the signature of $user_{i+1}$ can be add into the aggregate by using multiplication operation.

$$\sigma' = \sigma \times \sigma_{n+1} \qquad (1)$$

And if $user_j$ desires to disaggregate his signature σ_j from aggregate signature σ, the signature of $user_j$ can be remove from the aggregate by using division operation.

$$\sigma' = \sigma / \sigma_j \qquad (2)$$

If, however, only the messages, each user's public key, and the aggregate signature σ are known, recovering the individual signatures from the aggregate is hard. This hardness assumption is equivalent to CDH(Computational Diffie-Hellman) problem[5].

3. FLEXIBLE VIDEO AUTHENTICATION BASED ON AGGREGATE SIGNATURE

In this section, we describe our proposal in detail. To overcome the problem that verification problem of modified video contents, it can be possible to modify a generated video content signature. Simultaneously, the modification should be preserve a rights both of creator and modifier. To offer modification property, we are using a aggregate signature and appling it to H.264/AVC NAL unit.

3.1 The proposed scheme

The proposed video authentication scheme consists of five algorithms as aggregate signature : Key Generation, Signing, Verification, Aggregation and Aggregate Verification. First three are usual algorithms for generating and verifying each NAL unit signatures. To generate each NAL unit signature, the user selects a public and private key pair in Key Generation algorithm and signs each NAL unit using selected key pair in Signing algorithm. Generated each NAL unit signature can be used to verify authenticity of each NAL unit by using Verification algorithm.

Key Generation. For a user, pick random $x \xleftarrow{R} Z_p$, and compute $v \leftarrow g^x$. The user's public key is $v \in G$. The user's private key is $x \in Z_p$.

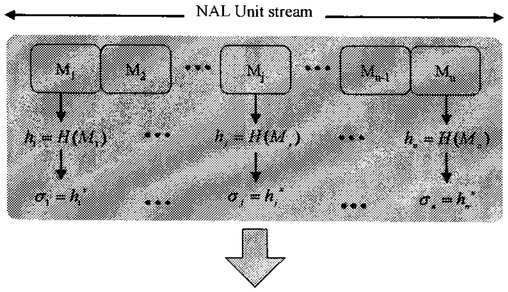
Signing. Given the private key x and a NAL unit $M \in \{0,1\}^*$, compute $h_i \leftarrow H(v,M)$, where $H \in G$, and compute $\sigma \leftarrow h^x$. The signature is $\sigma \in G$.

Verification. Given a user's public key v, a NAL unit M, and a signature σ, compute $h \leftarrow H(v,M)$ accept the validity of signature σ if $e(\sigma,g) = e(h,v)$.

Remaining two additional algorithms provide the aggregation capability. The aggregate signature is generated from each NAL unit signature by just multiplies all the NAL unit signatures and its size is same as short signature, half the size of 320-bits(DSA) long. So, the communicational cost is half compared with conventional digital-signature based video authentication. Moreover, it is secure that its security is belongs to aggregate signature. In the Fig. 4 shows the H.264/AVC NAL units and how to apply aggregate signature to the H.265/AVC NAL unit structure.

Aggregation. Each NAL unit signatures $\sigma_i \in G$ $(1 \le i \le n)$ on each NAL unit $M_i \in \{0,1\}^* (1 \le i \le n)$, aggregated into a content signature. Compute $\sigma \leftarrow \prod_{i=1}^{n} \sigma_i$. The content signature is $\sigma \in G$.

Aggregate Verification. Given an content signature $\sigma \in G$ for a NAL unit sequence, and the original NAL unit sequence M_i $(1 \le i \le n)$ and public



$$\sigma = \sigma_1 \cdot \cdots \cdot \sigma_n = \prod_{i=1}^{n} \sigma_i \quad (1 \le i \le n)$$

Fig. 4. Aggregate signature with H.264/AVC NAL unit

key v, To verify the content signature, compute $h \leftarrow H(v, M_i)$, and accept if $e(\sigma, g) = \prod_{i=1}^{n} e(h_i, v)$ holds.

Let consider that user Bob desire to modify a m_i from content $M = \{m_1, \ldots, m_n\}$ of user Alice. And the each NAL unit signature is the content sig nature of content M is $\sigma = \prod_{i=1}^{n} \sigma_i$. To modify a m_j, Bob have to receive individual content signature σ_j from Alice. However, disclosure of individual content signature may bring a serious affects on a system. Accordingly, a system should keeps individual content signature secure when transmitting a it through a opened channel.

In the Fig. 5 illustrates a communication that how to transmit a request patial NAL unit signature securely. When partial NAL unit signature σ_j was requested from Bob, Alice encrypts the partial NAL unit signature with Bob's public key ($E_{v_B}\{\sigma_j\}$) and transmits it to the Bob. Because of nobody can not decrypts the message without Bob's private key, encrypted partial NAL unit signature can be transmitted to Bob securely.

Transmitted partial NAL unit signature σ is used to remove individual content signature from content signature σ by using Eq. (2). And then generated new partial NAL unit signature σ_j from modified content(m'_j) added to content signature

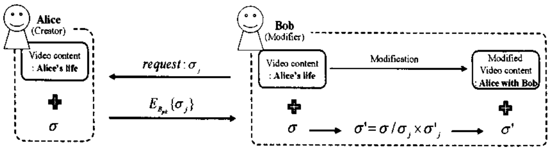


Fig. 5. Modification of video content

Modified content signature σ' can be used to verify integrity and to confirm right's of Alice and Bob. Given modified content $M' = \{m_1, \ldots, m'_j, \ldots, m_n\}$, generator g, Alice' public key v_B and Bob's public key v_B. Because, we can computes as :

$$\begin{aligned} e(e', g) &= e(h_1^{x_A} \times \cdots \times h_{j-1}^{x_A} \times h_j^{x_B} \times h_{j+1}^{x_A} \times \cdots \times h_n^{x_A}, g) \\ &= \prod_{i=1}^{j-1} e(h_i, g)^{x_A} \times \prod_{i=j+1}^{n} e(h_i, g)^{x_A} \times e(h_j, g)^{x_B} \\ &= \prod_{i=1}^{j-1} e(h_i, g^{x_A}) \times \prod_{i=j+1}^{n} e(h_i, g^{x_A}) \times e(h_j, g^{x_B}) \\ &= \prod_{i=1}^{j-1} e(h_i, v_A) \times \prod_{i=j+1}^{n} e(h_i, v_A) \times e(h_j, v_B) \end{aligned}$$

3.2 Application to UCC service

With a development of video coding technologies and devices, and revitalization of video content distribution services through the internet, anyone can make a video content and distribute it easily. UCC service is the representative model.

In UCC service, Fig. 6, there are three user's in a system Alice, Bob and Carol. The Alice who is generates content A and uploads to service provider. Bob is modifier want to modify Alice's content A. Carol can be general user or verifier. It is possible to modify the content A by Bob without any permission from Alice. If that, Carol cannot recognize the owner of content A. There is no way preserving Alice's right in general UCC services as aforementioned verification problem of modified video contents.

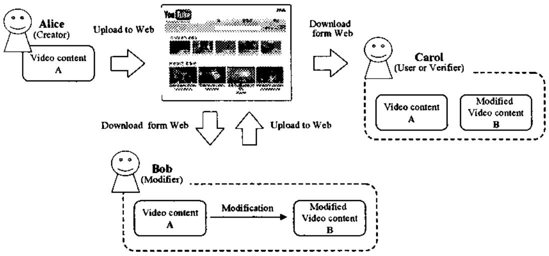


Fig. 6. Video content distribution on UCC service.

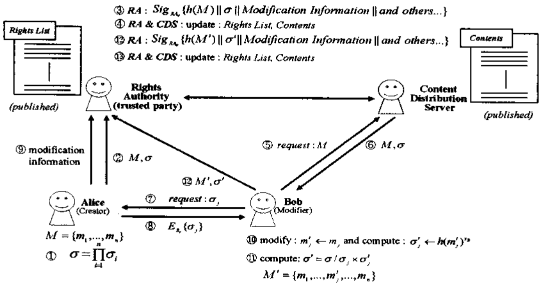

③ RA : $Sig_{RA_s}\{h(M)\|\sigma\|$ Modification Information $\|$ and others...$\}$
④ RA & CDS : update : Rights List, Contents
⑫ RA : $Sig_{RA_s}\{h(M')\|\sigma'\|$ Modification Information $\|$ and others...$\}$
⑬ RA & CDS : update : Rights List, Contents
Rights List
(published)
Rights Authority (trusted party)
Content Distribution Server
Contents
(published)
⑨ modification information
② M,σ
⑫ M',σ'
⑤ request : M
⑥ M,σ
Alice (Creator)
⑦ request : σ_j
⑧ $E_{B_s}\{\sigma_j\}$
Bob (Modifier)
$M=\{m_1,\ldots,m_n\}$
① $\sigma=\prod_{i=1}^{n}\sigma_i$
⑩ modify : $m'_j \leftarrow m_j$ and compute : $\sigma'_j \leftarrow h(m'_j)^{x_B}$
⑪ compute: $\sigma'=\sigma/\sigma_j\times\sigma'_j$
$M'=\{m_1,\ldots,m'_j,\ldots,m_n\}$

Fig. 7. Video content distribution on UCC service with proposed scheme.

To overcome this problem, we constructs a new UCC distribution service model. In this model, Fig. 7, content A is signed using algorithm Signing and Aggregation by Alice before updating to the Content Distribution Server(CDS) and Rights Authority(RA). RA and CDS can be located same domain. If RA received content A from Alice, it generates Binding Information(Certification of content, Fig. 7. ⑬) to make Rights Lists(RL) that is used to provide certification of contents for users. Only a content which is generated RL can be distribute through the CDS.

If Bob desire to modify the content A, he can be download it from CDS and modify the content A, but he must be permitted from Alice to modify the content signature.

After the modification of content A, there are two contents on CDS. If Carol downloads a content A or modified content B, she can verify the downloaded content by the use of algorithm Aggregation Verification with RL.

4. DISCUSSION

In this paper, 'flexibility' means that how to modify a content and content signature easily and securely. Conventional video authentication schemes are not suitable for aforementioned verification problem of modified video content.

It is possible to solve the problems using conventional video authentication. One solution is that use two or more content signatures. However, using two or more content signatures is not proper way owing to efficiency. In modifier side, if he wants to recreate a part of video content using conventional video authentication schemes, he should be access whole part of a video content. It will be caused inconvenience to authenticated modifier.

Another problem of using several content signature is complexity of management. If there are two or more signature on one content, RA should have more information about those content signature and more storage to store all signatures.

We are using just one content signature by using of aggregation of partial content signature. Partial content signature are easily added or removed and it brings efficiency of video content modification. In modifier side, just partial parts of video content signature can be generated. Modifier need not to consider about other part of video content. And generated just one content signature.

Table 1. shows comparison of video authentication schemes. In digital-signature based video authentication, integrity refers to the whole video data; even data with a one-bit alteration will be claimed as unauthentic. Therefor no robustness is required. The main concern is the security of the authentication scheme. Such criterion motivates researches to develop signature-based complete

Table 1. Comparison of video authentication schemes

	Digital signature-based[3,11]	Media signature-based[12]	proposed scheme
Content integrity	Yes	Yes	Yes
Robustness	No	Yes	No
Signature size	Short	Large	Very Short
Security	Strong	some	Strong
Signature Modification	Impossible	Impossible	Possible

authentication scheme whose security level is very high and can be proven mathematically. And the size of signature belongs to a appropriated cryptographic authentication algorithm.

In media-signature based video authentication, integrity refers to the content of the video data; the video content is considered authentic as long as the meaning of the video data remains unchanged. Therefore, besides the security requirement, a certain level of robustness to distortions is required. The main concern is how to extract a feature from a video content. However, because of only a part of video content is used for a feature extraction, extracted feature can not cover whole part of video content. And also, feature extraction dose not proved mathematically or cryptographically so far.

Proposed scheme to be classified into digital signature-based video authentication. Therefore general properties are same as digital signature-based video authentication except 'signature size' and 'signature modification'. Proposed scheme based on short signature and aggregate signature. Consequently, proposed scheme has half size of Digital Signature Algorithm (DSA) with comparable security and signature can be modify securely. However, our proposed scheme cannot be directly use to real video coding standard reason of references such as motion estimation and compensation. Modification of one NAL unit or access unit may cause propagation to other NAL units and access units when decompress a coded video stream.

Proposed scheme can be applied not only UCC service but also other applications. For example, joint production of content environment that two or more users participated in creating a content is possible scenario. Collaborated users generates each content signature, and then generated each content signatures are can be aggregated. All the users can confirm own rights on joint produced content.

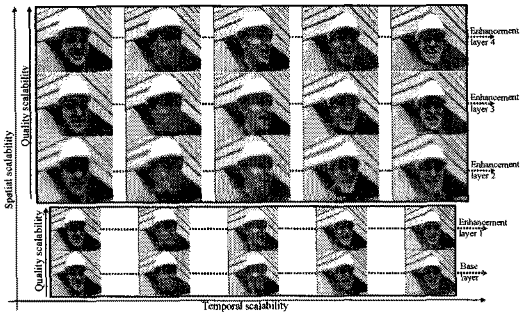


Fig. 8. Overview of SVC layer structure.

Besides of flexibility, proposed scheme can be applied to scalable coding. Coded video stream can be divided into several layers. This technique is called scalable video coding(SVC)[11] and it consists of compressing a digital video into a single bitstream in such a way that other meaningful and consistent can be generated by discarding parts of the original compressed stream. Those sub-stream can be directly interpreted at different bitrates, different resolutions or different time scales. Fig. 8 illustrates overview of SVC layer structure.

Because of each scalable levels are also transmitted forms of NAL unit, access unit, proposed scheme can be applied into the SVC depending on requirements of users. We can define each level and each layer content signatures.

5. CONCLUSIONS AND FUTURE WORKS

In this paper, we defined verification problem of modified video content and proposed a new authentication that flexible use of content to overcome the problem. To provide authenticity of a digital video contents and property of modifiable signature, we used aggregate signature that is one of cryptographic signature based on short signature. Advantage of our scheme is that modification of signed video content is allowed if necessary and can guarantee rights of all collaborated users. Moreover, the aggregated signature has half size in comparison with DSA.

However, our proposed scheme cannot be directly use to real video coding standard reason of references such as motion estimation and compensation. Modification of one NAL unit or access unit may cause propagation to other NAL units and access units when decompress a coded video stream. So, we have to consider suitable packetizaion scheme which guarantees non-propagate property of other packets.

REFERENCES

[1] W. Zeng, H. Yu, and C. Lin, Multimedia Security Technologies for Digital Rights Management, Elservier Inc, London, UK., 2006.

[2] Q. B. Sun and S.-F. Chang, Multimedia Security HandBook, CRC press, Boca Raton, FL, 2004.

[3] C.-Y. Lin and S,-F. Chang. "Issuse and solutions for authenticating MPEG video," SPIE Int. Conf, Security and Watermarking of Multimedia Contents, Vol.3657, No.06, pp. 54-56, 1999.

[4] ITU-T Recommendation H.264, "Advanced video coding for generic audiovisual services," 2005.

[5] Atul Puri, Xuemin Chen and Ajay Luthra. "Video conding using the H.264/MPEG-4 AVC compression standard," Signal Processing : Image Communication, No.19, pp. 793-849, 2004.

[6] T. Wiegand, Gary J. Sullivan, G. Bjøntegaard, and A. Luthra. "Overview of the H.264/AVC Video Coding Standard," IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No.7, 2003.

[7] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," Eurocrypt 2003, LNCS 2656, pp. 416-432, 2003.

[8] D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the Weil pairing," Proceedings of Asiacrypt 2001, LNCS 2248, pp. 514-532, 2001.

[9] A. Menezes, P. Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, 1996.

[10] D. Boneh, C. Gentry, B. Lynn and H.Shacham. "A Survey of Two Signature Aggregation Techniques," RSA CryptoBytes, Vol.6, No.2, pp. 1-9, 2003.

[11] Yu, H., "Scalable Multimedia Authentication," the 4th IEEE Pacific-Rim Conference on Multimedia (PCM) 2003, Vol.1, pp. 443-447, 2003.

[12] Q. Sun, D. He, Z. Zhang, Q. Tian, "A secure and robust approach to scalable video authentication," International Conference on Multimedia and Expo'03, Vol.2, pp. II-209-212, 2003.

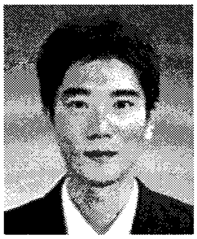
[13] Heiko Schewarz, Detlev Marpe and Thomas Wiegand, "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," IEEE Transaction on Circuits and Systems for Video Technology, Special Issue on Scalable Video Coding, Vol.17, No.3, pp. 1103-1120, 2007.

Shin, Weon

received the M.S. and Ph.D. degrees from Pukyong National University. Busan. Korea in 1996 and 2001, respectively. From March 2002 until January 2005 he worked to develop security softwares and led the development process for security softwares as a senior researcher in AhnLab, Seoul, Korea. He is currently a Assistant Professor in the Department of Information Security, Tongmyong University, Busan, Korea. His research interests are in the areas of software security, reliable P2P computing and security applications.

Hong, Young-Jin

received the B. S. E. E. degree from Seoul National University. Seoul. Korea, in 1978 and the M. S. E. E. and Ph. D.(E. E.), from the State University of New York at Stony Brook in 1982 and 1985, respectively. From January 1986 until May 1986 he was with the Department of Electrical Engineering at the State University of New York ay Stony Brook, as an Assistant Professor. In June 1986 he joined LNR Communications, Inc., Hauppauge, NY, where he was a Research Staff Engineer and working on spread spectrum systems and satellite communications. In 1992 he came back to Korea to join Samsung Advanced Institute of Technology(SAIT), where he had been leading several research projects including CT2, VSAT and TDMA cellular basestations for two years. Since then he has broadened the spectrum of his career path to include not only the area of R&D(CTO of Eastel Systems from 1994 through 1997; CTO of Sungil Telecom in the year of 2004) sector but also the business area(executive managing director of SKC&C from 1997 to 2003). He is currently an Associate Professor in the Department of Electrical and Electronics Engineering, Tongmyong University, Busan, Korea. His research interests are in the areas of smart antenna system, adaptive signal processing and communication systems. Dr. Hong is a member of Korean Institute of Communication Sciences, The institute of Electronics Engineers of Korea. he is also a member of IEEE.



Lee, Won-Young

received the B.S. degree from Pukyong National University. Busan. Korea in 2007. and the M.S. degree from Pukyong National University. Busan. Korea in 2009. His research interests are in the areas of information and multimedia security.

Kyung-Hyune Rhee

received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology, Daejon Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute, Daejon Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide, Australia, the University of Tokyo, Japan, Kyushu University, Japan, and the University of California, Irvine, U.S.A. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a Professor in the Division of Electronic, Computer and Telecommunication Engineering, Pukyong National University, Busan Korea. His research interests center on key management, mobile communication security, multimedia security, DRM and cryptographic algorithms, etc.