Content Sharing between Home Networks by using Personal Information and Associated Fuzzy Vault Scheme

Hosik Sohn, Yong Man Ro, *Senior Member*, IEEE, and Kostantinos N. Plataniotis, *Senior Member*, IEEE

Abstract — *Content sharing is getting popular in home network as well as in social media. Content sharing inside home is usually done among family members, while that between different home networks is done by friends and even anonymous users. Especially, anonymous users could access contents in home networks which could act like home portals. To protect content in home servers, the contents can be encrypted by key and the key can be shared among users. However it is quite challenging to distribute the key to anonymous users. In this paper, we present a method for sharing contents securely among different home networks. We propose a method of content sharing between anonymous users, who have similar personal preferences about the contents. The personal preferences include user profiles and contents preference. With the proposed method, a content sharing community is created for content delivery between different home networks. The community allows content creators to deliver contents to other users, who have similar personal information and can consume the contents without any leakage of personal information. In order to verify the usefulness of the proposed method, experiments were performed. The results showed that contents in one home server were securely shared with users of the other home server, if both have similar personal information.*

Index Terms — UGC, Content sharing, home network, personal information

I. INTRODUCTION

The number of user generated contents has been rapidly increasing during the last couple of years [1]-[3]. Ordinary people have become producers of contents as well as consumers so called "prosumers", being capable of publishing their own contents. As user content generation is getting more convenient, content sharing through home network as well as through social media is getting popular. People can share contents inside and even outside the home with diverse devices using home networks. Each Home can be the core of content generation, edition, and sharing, and anonymous users can access contents in the home network which can act like content portals [4].

Hosik Sohn is with the Image and Video System Lab, Information and Communications University (ICU), Daejeon, Republic of Korea (e-mail: sohnhosik@icu.ac.kr)

Prof. Yong Man Ro is a director of the Image and Video System Lab, Information and Communications University (ICU), Daejeon, Republic of Korea (e-mail: yro@icu.ac.kr)

Prof. Konstantinos N. Plataniotis is a professor of Electrical and Computer Engineering at the University of Toronto, Canada (e-mail: Kostas@comm.utoronto.ca)

Contributed Paper
Manuscript received November 13, 2008

The increasing availability of high speed network access and the tendency of decreasing cost of personal storage, triggers the need for content sharing among different home networks as well as within a home [5], [6]. Content sharing can be done among family members, friends, and even anonymous users. For the family members and acquaintances, the full right to access contents could be granted so that they can freely consume the contents inside or outside the home.

However, for the case of anonymous users, since there is no relationship or acquaintanceship between the users, i.e., content consumers, and content creators, the content creators will be concerned about delivery to unwanted group of people and the misusage of contents. Therefore, the content creator would like to give a restriction to the access of contents and share his/her contents with only the group of people who have similar personal preferences about the contents, such as user profile and content preference. (e.g., people who have same occupation, hobby, and favorite movie).

Specifically, if the contents are encrypted by a key and the key is distributed to the preferred group of people, content creators would not be concerned about the misusage of their contents. However, it is not easy to distribute the key to anonymous users who have a similarity in terms of user profile and content preference. Private concerns might come up: During the process of measuring the similarity of personal information, user's personal information could be revealed to another user.

There should not be any revelation of personal information during the comparison of personal information between anonymous users and content creators. The personal information of users such as name, gender, date of birth, religion, occupation, and hobby should be private. Users would like to hide their personal information in the public. In fact, revealing personal information on the Web could cause various security related attacks [7].

In this paper we propose a new scheme which allows users to share contents securely among different home networks. By the proposed method, a content sharing community between different home networks could be available for users whose personal information is similar. In order to create such community, we have used the vault set that is an encoding result of fuzzy vault scheme [8]. By applying the fuzzy vault scheme, the personal information of users can be kept secured during the process of the proposed method.

Fuzzy vault scheme had been introduced to provide security using biometric data such as finger print and face features [9]-[11]. The concept of fuzzy vault is that the vault set is generated through binding both biometric data and the secret key, and the generated

vault set provides the secret key only if it is decoded with the identical biometric data. The biometric data of users should not be revealed to other people. In the light of the aforementioned in Fuzzy vault, this paper proposes a content sharing method with fuzzy vault scheme using personal information.

The rest of the paper is organized as follows: Section 2 provides content sharing method based on personal information among home networks. Section 3 explains the process of transforming personal information to binary and encoding/decoding of the vault set using the personal information. The experiments and results are presented in section 4. Finally, section 5 concludes the paper.

II. Content Sharing based on Personal Information among Different Home Network

Home server in home network grants access right to a group of people in accordance with acquaintance. The group of people could be classified into family, friends, and visitors. Family and friends could represent trusted people. For the trusted group like family and friends, full access rights could be granted with authentication key so that they could access contents with their own devices with access rights given by home content creator. The visitors could represent anonymous people who want to access home server and consume contents. Though there is no relationship or acquaintanceship between visitors and the content creator, the content creator would like to share his/her contents with people who have a similarity such as user profile or content preference.

In the proposed system for content sharing in home networks, contents are encrypted with a secret key. The secret key is granted to family and friends for free contents consumption. However, for the case of visitors, secret key is granted based on comparison of personal information. If visitor's personal information is similar with that of content creator, the visitor can acquire the secret key and decrypt the content for consumption.

The type of connection to home server is classified into local and remote connectivity based on the connection spot. The local connectivity to home is established using UPnP [12] audio/video (AV) control point (CP). Control Point and UPnP devices are compared to client and server. The CP controls the UPnP devices to transmit contents and find UPnP devices. The remote connectivity to home can be feasible using virtual private network (VPN) [13]. VPN guarantees the secure tunnel between a visitor and home server.

Fig. 1 represents visitor's remote connection to home server. This figure shows how the visitor accesses from outside the home. Content creator (home server side) is a user who wants to open the content to the group of people who have similar personal information. The creator encodes a vault set with personal information of preferred visitor (PI_p) and secret key (K). The vault set (VS) is generated by binding the personal information and secret key. The contents are encrypted by the secret key and opened to public along with the vault set. C^e in the figure represents encrypted content.

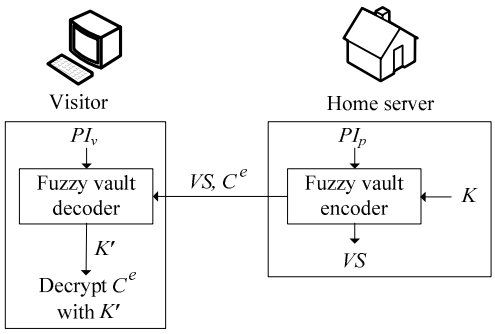


Fig. 1. Content consumption process with Vault set in home network.

A Visitor is a user who wants to consume the content of home server. In order to consume the content, the visitor downloads vault set (VS) and decodes it with his/her personal information (PI_v). The decoding result of vault set is secret key (K'). Therefore, if the visitor's personal information is overlapped as many as the content creator wants, he/she can acquire identical secret key (K') with original secret key (K). Then, visitor can decrypt the encrypted content and consume it. Since the access to the encrypted contents are given to visitors according to their personal information (user profile and content preference), home servers with similar personal information can be defined as a group, i.e. community. This space, generated by the vault set, is only opened to visitors with similar personal information. Thus, the community can be secured by grouping the contents according to personal information. Grouped communities according to similar preferred personal information is depicted in Fig. 2.

From the perspective of home server, this could provide limited accessibility to the unpreferred visitors. The benefit of applying fuzzy vault scheme to content sharing is as follows: It is possible to share contents even though personal information between users is not perfectly matched, and the proposed system does not require a centralized authority that deals with private information and secret key of home servers. The only function of authority is to distribute user profile/content preference table (will be mentioned in section III.B) and open the contents along with vault set.

If the personal information is encrypted without utilizing fuzzy vault scheme, the centralized authority is required to deal with key management and distribution. The security of centralized authority should be guaranteed as well. In practice, key management is the difficult aspects of cryptography. Moreover, in order to compare user information among other users, encrypted personal information should be transformed to the same domain or decrypted to original information.

For the case of transforming to the same domain, the knowledge of rules that transform encrypted personal information by different keys into the identical domain for comparison is required of the authority. If the encrypted personal information is decrypted to original information, the personal information is revealed at other visitors' side or open home server side. In the practical standpoint, the perfect security in the centralized authority cannot be guaranteed. Also, vulnerable authority has a risk of revealing all personal information at once.

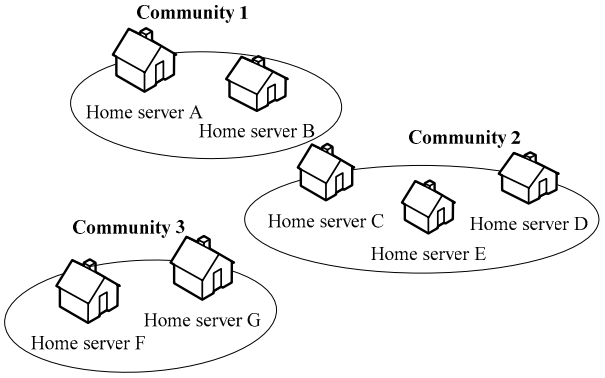


Fig. 2. The community generated by personal information.

In the next section, the a fuzzy vault scheme to generate content sharing community is presented, where personal information is secured as well as secure delivery and consumption of contents are guaranteed.

III. FUZZY VAULT SCHEME USING PERSONAL INFORMATION

In this section, detailed explanation of encoding and decoding procedure in Fuzzy vault scheme using personal information is presented. Vault set is generated by binding the personal information of home server user and a secret key which is used for protecting the content.

In order to consume the contents, consumer should decode the vault set by his/her personal information. If certain number of personal information matches personal information of consumers, then the proper secret key is acquired, and finally consumers can decrypt or access the content. Before explaining encoding and decoding procedure, we define the personal information item of user (binarized personal information), and describe how to generate it.

A. Quantification of personal information: User Information Item (UII)

In order to use personal information as an input of fuzzy vault scheme, we define personal information items such as age, gender, and favorite contents. Table 1 represents the defined personal information items used in this paper. The personal information consists of user profile and content preference. The classification scheme (CS) of MPEG-7 user preference [14] was referred to make Table 1.

In addition, hobbies [15] and occupation [16] sections were appended to define the personal information. As is seen in Table 1, user profile and content preference have sub-items. The number inside Table 1 denotes the number of attribute of sub-items. User profile consists of items related to personal information, such as age, gender, occupation, and hobby. Content preference contains items that can represent the user's favorite contents, such as drama, music, and movies.

TABLE I
USER PROFILE/CONTENTS PREFERENCE TABLE

User information	Subcategory (P_i, i=1 to 288)
User profile	Age (6), Gender (2), Marriage status (4), Hobby (23), Occupation (24), Language (139)
Contents preference	Information (13), Drama (14), Entertainment (25), Music (10), Enrichment (11), Movies (17)

To use the mentioned personal information items as an input of fuzzy vault scheme, each item is assigned to 16 bit-value. Namely, in order for sub-items in Table 1 to be used as an input of fuzzy vault scheme, we assigned 16 bit-pseudo-random number to each item as presented in Fig. 3.

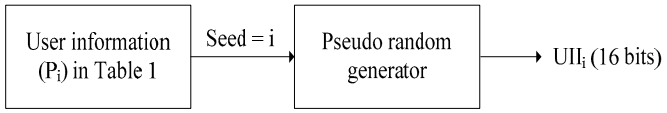


Fig. 3. Binalization of user information.

We defined this value as user information item (UII). N number of UIIs corresponding to his profile and content preference at the encoder and decoder side is used as an input. Let the set of UII at the encoder side be the $T=\{t_1, t_2,\ldots,t_N\}$, and at the decoder side be the $Q=\{q_1, q_2,\ldots,q_N\}$.

B. Fuzzy vault encoder with UII

Fig. 4 represents the fuzzy vault encoder using user information item, UII. As seen in the figure, fuzzy vault encoder generates a vault set with the list of UII and secret key as an input. User's UIIs are generated through the procedure of Fig. 3 with N number of items P_i of table 1. The set of user's UII is $T=\{t_1, t_2,\ldots,t_N\}$ which is identical to template user information item list, T in Fig. 4.

128-bit Advanced Encryption Standard (AES) key is used as a secret key to protect the contents [17]. Through Cyclic Redundancy Check (CRC), 16 bit redundancy is added to the secret key. For generating cyclic redundancy, CRC-16 scheme, which has 16-bit primitive polynomial, is used [18].

$$g_{CRC}(a) = a^{16} + a^{15} + a^2 + 1 \tag{1}$$

Through CRC encoding, 16-bit redundancy is added to 128-bit AES key so that total of 144-bit data SC is constructed. In order to construct polynomials of (2), SC is divided into non-overlapping 16-bit unit and used to generate coefficients (C_8 to C_0) of polynomial. Every operation after the construction of polynomial is under the Galois field ($GF(2^{16})$).

$$p(u) = c_8 u^8 + c_7 u^7 + \cdots + c_1 u + c_0 \tag{2}$$

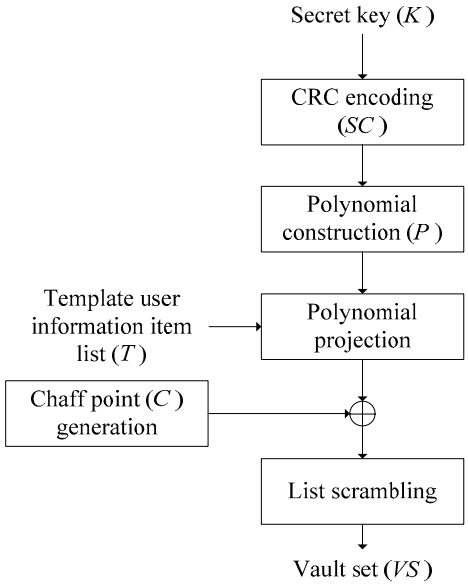


Fig. 4. Schematic diagram of fuzzy vault encoder.

A vault set, which is the encoding result, consists of genuine set G and chaff set C. The elements of genuine set are a pair of values, which is a template of user information item list $T=\{t_1, t_2,\ldots,t_N\}$ and its projected value to polynomial $p(u)$ of (2). Genuine set G is expressed as (3).

$$G=\begin{Bmatrix}(t_1, p(t_1))\\(t_2, p(t_2))\\\vdots\\(t_N, p(t_N))\end{Bmatrix} \tag{3}$$

And chaff set C can be defined as (4).

$$C=\begin{Bmatrix}(u'_1, d_1)\\(u'_2, d_2)\\\vdots\\(u'_M, d_M)\end{Bmatrix} \tag{4}$$

Chaff set C is used to protect the genuine set securely. Chaff set C is composed of M number of UIIs ($u'_1, u'_2,\ldots,u'_M$) from 288 UIIs in user profile/contents preference table 1 ($u'_i \neq t_j$, for $1 \le i \le M$, $1 \le j \le N$), which are not used as personal information. The values satisfying (5) is chosen for d_1 *to* d_M.

$$p(u'_i) \neq d_i \quad 1 \le i \le M \tag{5}$$

Then, even if the adversary (malicious attacker) knows user profile/contents preference table, the attacker cannot distinguish between genuine set and chaff set. Finally, the vault set VS is generated by scrambling the genuine set G and chaff set C.

$$VS=\begin{Bmatrix}(v_1, w_1)\\(v_2, w_2)\\\vdots\\(v_{N+M}, w_{N+M})\end{Bmatrix} \tag{6}$$

C. Fuzzy vault decoder with UII

The fuzzy vault decoder uses UIIs as an input and if more than D+1 number of UIIs is the same as that of encoding side, the original secret key can be acquired which guarantees the successful decryption of the content. Here, D denotes the degree of polynomial in (2). Query UIIs are generated through the procedure of Fig. 3 with N number of UII from items (P_i). The set of user's UII is $Q=\{q_1, q_2,\ldots,q_N\}$, which is identical with Query user information item list Q in Fig. 5.

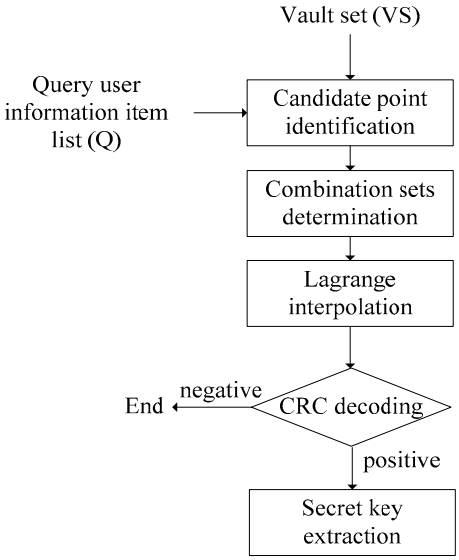


Fig. 5. Schematic diagram of fuzzy vault decoder.

The element of VS, (v_j, w_j) which satisfies the (7), is selected as a candidate point after comparing query UIIs and elements of the vault set.

$$q_i = v_j,\ 1 \le i \le N,\ 1 \le j \le N+M \tag{7}$$

If the number of candidate points is k, the next step "Combination sets determination" generates every possible set that can select D+1 number of points from k number of candidate points, $C(k, D+1)$. Let each set be the $L=\{(x_1, y_1), (x_2, y_2),\ldots,(x_{D+1}, y_{D+1})\}$, then the polynomial is reconstructed using (8) for case of $C(k, D+1)$ in Lagrange interpolation block.

$$p^*(u)=\sum_{j=1}^{D+1} y_j p_j(u) = c_8u^8 + c_7u^7 + \cdots + c_1u + c_0$$
$$\text{where } p_j(u)=\prod_{i=1, i\neq j}^{D+1}\frac{u-x_i}{x_j-x_i} \tag{8}$$

In order to construct *SC** of 144 bits data, the coefficients C_0 *to* C_8 obtained by (8) are concatenated. Every *SC** checks the redundancy through CRC decoder. And if the redundancy is not zero, the result of CRC decoding is negative. Thus, it is impossible to acquire the proper secret key. Therefore, in the case of redundancy being zero, only 128 bits excluding LSB 16 bits are used for decrypting the content.

IV. Experiment and Discussion

Experiments were performed to verify the proposed content sharing between home networks by using personal information. In the experiments, the consumption process for protected contents with vault set developed by personal information is evaluated. Through content sharing using personal information, we demonstrated a content sharing community among home servers in which protected contents could be shared. Fig. 6 shows the detail experimental scenario.

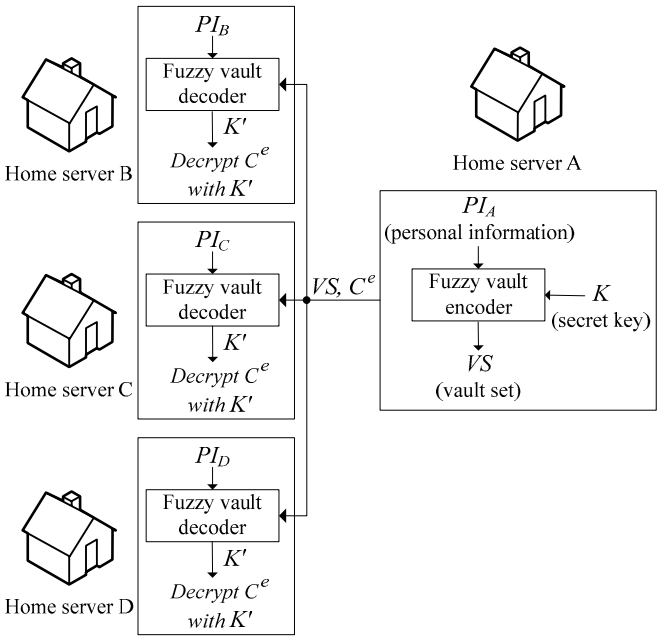


Fig. 6. Experiments scenario. Notes Home server A produces encrypted content C^e and associated vault set by using personal information of home server A user.

We established four home servers. Four home server users were named as A, B, C, and D, respectively. Users of home server B, C, and D accessed the encrypted content of home server A. The home server A generated encrypted contents with the vault set and opened them to the public so that the rest of home servers could consume them.

Detailed personal information of four home servers used in the experiment is presented in Table 2. As seen in Table 2, home server user B has 8, home server user C has 9 and home server user D has 10 identical personal information with home server user A, respectively. Note that home server A had encrypted contents and vault set generated by the personal information of home server A user. We want to observe whether home server users B, C, and D, who have different personal information, could decrypt and consume the encrypted content of home server A.

TABLE II
Personal Information of Home Server A, B, C and D in the Experiment

User information	Sub-category	Home server A	Home server B	Home server C	Home server D
User profile	Age	Young Adults	Senior citizens	Young adults	Senior citizens
	Gender	Male	Male	Female	Female
	Marriage status	Single	Single	Single	Single
	Hobbies	Photography	Collecting	Photography	Photography
	Occupation	Computer and Mathematical	Computer and Mathematical	Legal	Computer and Mathematical
	Language	English	English	English	English
Contents preference	Information	Social/Political	Sport events	Social/Political	Social/Political
	Drama	Docudrama	Docudrama	Docudrama	Docudrama
	Entertainment	Quiz/Contest	Travel variety	Quiz/Contest	Quiz/Contest
	Music	Jazz	Jazz	Jazz	Jazz
	Enrichment	Language studies	Language studies	Language studies	Language studies
	Movies	Effect movies	Effect movies	Horror	Effect movies

Table 3 is the fuzzy vault decoding result for home server user B, C, and D with the vault set encoded by home server user A. Because the number of user's personal information was 12, the number of candidate set generated at the decoder size was 220 which was the number of possible combination of selecting 9 from 12 ($C(12, 9)$).

TABLE III
Decoding Result

Visitor to home server A	Candidate points		Decoding result	
	Number of matched to genuine user's UII	Number of matched to chaff points	Number of positive set in CRC decoding	Number of negative set in CRC decoding
Home server user B	8	4	0	220
Home server user C	9	3	1	219
Home server user D	10	2	10	210

In Table 3, the number of positive set represents the number of sets where the redundancy is zero in CRC decoding in Fig 5. Likewise, the number of negative represents the number of sets where the redundancy is not zero. If the CRC decoding result is positive, the probability of a set containing the proper secret key is very high while the set has no secret key in the case of result being negative. The decoding process was finished as soon as the secret key was found, and encrypted content was decrypted by the key.

As seen in the experimental results of Table 3, home server user B could not access the content of home server A.

Eight identical UIIs to home server user A are not enough to reconstruct a polynomial so that proper secret key could not be acquired. For home server C, 9 UIIs are identical to home server A. Thus, only one set ($C(9, 9)$) out of 220 is positive in CRC decoding. For home server D, since 10 UIIs are identical to home server A, 10 sets ($C(10, 9)$) are positive in CRC decoding. Therefore, home server C and D could decrypt the protected content of home server A with secret key which is a 128-bit from MSB of 144-bit SC^* in Fig 5.

The experimental results shown above, can explain a content sharing community generated by personal information, which is opened to home server user A, C, and D, but not to home server user B. Since home server user A, C, and D have more than 9 identical personal information items each other, the encrypted content of each home server could be decrypted with the vault set generated by their own personal information. As shown in Fig. 7, it means a content sharing community could be created so that home server A, C, and D can upload their contents freely and share them securely while home server B can not access.

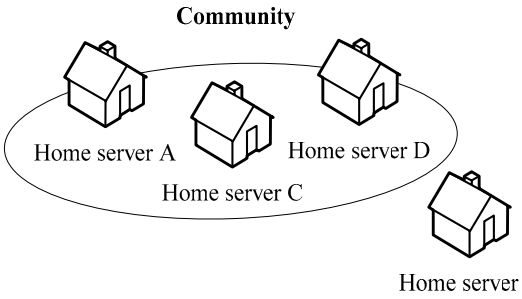


Fig. 7. A content sharing community generated by personal information.

For the security considerations in the experiment, let us assume that an adversary wants to break the content sharing community using brute force attack simulated by our experimental environment, i.e., iterating over all combinations of attributes and try to access the virtual space by randomly selecting 9 UIIs from 12 sub-categories where only one UII is selected for each sub-category. For a given user profile/content preference table shown in Table 1, the adversary could break the virtual secure space by evaluating all combination sets (8.8×10^{12} sets) at maximum.

V. CONCLUSION

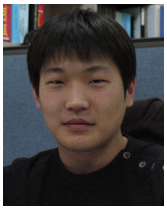
With the increasing demand for building home network, content sharing among different home network becomes necessary as well as the sharing within a home. Further, each user's home can function as the contents' portal. Though there may be no relationship or acquaintanceship between users of different home networks, the content creator would like to share his/her contents with people who have similarities such as user profile or content preference.

The proposed method is to encrypt the content by secret key and open it to the public along with vault set that is generated by personal information of users. Since consumers, who have similar personal information to that of the content creator, can acquire the proper secret key, the content creator can limit the consumption of contents over group of consumers by his/her intention. The first priority to take into consideration in content sharing based on personal information is a risk of personal information leakage while comparing with other personal information. During the process of comparing personal information among users, no information is revealed to the public using fuzzy vault scheme.

Moreover, the proposed system does not require a centralized authority. Since the authority does not manage users' personal information, the resistance against personal information leakage is strong in the systemic view. Revealing of users' personal information all at once is not possible. With the proposed method, not only UGC creator can protect his content indirectly, but also increases the trust for the consumers of the contents.

REFERENCES

[1] OECD study on the Participative Web : User Generated Content, 3 October 2007. http://www.oecd.org
[2] M. Ames and M. Naaman, "Why We Tag: Motivations for Annotation in Mobile and Online Media," *in Proc. of CHI 2007*, San Jose, CA, USA, 2007.
[3] V. Loia, W. Pedrycz, and S. Senatore. "Semantic Web Content Analysis: A Study in Proximity-Based Collaborative Clustering," *IEEE Trans. on Fuzzy Syst.*, Vol. 15, Issue 6, pp.1294-1312, Dec. 2007.
[4] P. Belimpasakis and R. Walsh, "User Created Content in the Extended Home," *in Proc. of the 15th IST Mobile & Wireless Communication Summit*, Myconos, Greece, June, 2006.
[5] J. Walker, O.J. Morris, and B. Marusic, "Share It! - The architecture of a rights-manages network of peer-to-peer set-top-boxes," *in Proc. of EUROCON*, 2003.
[6] H. Y. Lee AND J. W. Kim, "An Approach for Content Sharing among UPnP Devices in Different Home Networks," *IEEE Trans. On Consum. Electron.*, Vol.53, Issue 4, PP.1419-1426, Nov. 2007.
[7] R. Gross and A. Acquisti. "Information revelation and privacy in online social networks," *in Proc. of ACM WPES*. Alexandria, VA, USA, pp. 71-80, 2005.
[8] A. Juels and M. Sudan. "A fuzzy vault scheme," *IEEE International Symposium., Information Theory*. pp.408-, 2002.
[9] K. Nandakumar, A. K. Jain, and S. Pankanti. "Fingerprint-Based Fuzzy Vault : Implementation and Performance," *IEEE Transactions., Inf. Forensics and Security*, Vol. 2, Issue 4, pp.744-757, Dec., 2007.
[10] Y. Wang, and K. N. Plataniotis. "Fuzzy Vault for Face Based Cryptographic key Generation," *Biometrics Symposium*, pp.1-6, Sept., 2007,
[11] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim. "Biometric key Binding: Fuzzy Vault Based on Iris Images," *Lecture Notes in Computer Science*, Vol. 4642/2007, pp.800-808, Aug., 2007.
[12] Universal Plug and Play, http://www.upnp.org/
[13] Cisco, "How Virtual Private Networks Work", http://www.cisco.com/warp/public/471/how_vpn_works.shtml
[14] ISO/IEC JTC1/SC29/WG11, Information Technology - Multimedia Content Description Interface - Part 5: Multimedia Description Schemes, FDIS(N4242), Nov. 2001.
[15] Wikipedia, List of hobbies.http://en.wikipedia.org/wiki/List_of_hobbies
[16] U.S. Department of Labor, Bureau of Labor Statistics. Standard Occupational Classification(SOC) Major Groups, http://www.bls.gov/soc/soc_majo.htm
[17] NIST. Advanced Encryption Standard (AES). Nov. 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[18] Press, W.H., Teukolsky, S.A., Vetterling, W.T. and Flannery, B.P. Numerical Recipes in C, Cambridge University Press, Cambridge, Second edition, 1992.



Hosik Sohn received the B.S. degree from Korea Aerospace University, South Korea, in 2007 and he is currently working toward the Ph.D. degree in the Information and Communications University (ICU), Daejon, South Korea. His research interests include bio-cryptography, H.264/AVC, scalable video coding, video adaptation, and visual quality measurement.

Yong Man Ro (M'92-SM'98) received the B.S. degree from Yonsei University, Seoul, South Korea and the M.S. and Ph.D. degrees from the Korea Advanced Institute in Science and Technology (KAIST), Daejon, South Korea. In 1987, he was a Researcher at Columbia University, and from 1992 to 1995, he was visiting researcher in University of California at Irvine and KAIST. In 1996, he was a Research Fellow, University of California at Berkeley. He is currently professor and director of Image Video System Laboratory in Information and Communications University (ICU). He participated in international standardizations including MPEG-7 and MPEG-21, where he contributed several MPEG-7 and MPEG-21 standardization works including MPEG-7 texture descriptor and MPEG-21 DIA visual impairment descriptors and modality conversion. His research interests include image/video processing, multimedia adaptation, visual data mining, image/video indexing, and multimedia security. Dr. Ro received the Young Investigator Finalist Award of ISMRM in 1992 and the Scientist Award (Korea) in 2003. He served a co-program chair of IWDW 2004.

Konstantinos N. Plataniotis (S'90-M'92-SM'03) received his B. Eng. degree in Computer Engineering & Informatics from University of Patras, Greece and his M.S. and Ph.D. degrees in Electrical Engineering from Florida Institute of Technology (Florida Tech), Melbourne, Florida. He was with the Computer Science Department at Ryerson University, Ontario, Canada from July 1997 to June 1999. Dr. Plataniotis is currently a Professor with The Edward S. Rogers Sr. Department of Electrical and Computer Engineering at the University of Toronto in Toronto, Ontario, Canada, where he directs the Multimedia Laboratory. He is also an Adjunct Professor with the School of Computer Science at Ryerson University. Kostas is a founding member and the inaugural Associate Director – Research of the Identity, Privacy and Security Initiative (IPSI) at the University of Toronto. He serves on the Executive Committee of Knowledge Media Design Institute (KMDI) at the University of Toronto. Dr. Plataniotis was the Guest Editor for the March 2005 IEEE Signal Processing Magazine special issue on Surveillance Networks and Services, and the Guest Editor for the EURASIP Applied Signal Processing Journal's special issue on "Advanced Signal Processing & Pattern Recognition Methods for Biometrics". Kostas is an Associate Editor for the IEEE Transactions on Neural Networks and the IEEE Signal Processing Letters. He is a member of the 2008 IEEE Educational Activities Board and the Chair of the IEEE EAB Continuing Professional Education Committee. Dr. Plataniotis is the 2008 representative of the Computational Intelligence Society to the IEEE Biometrics Council, and a member of the Steering Committee for the IEEE Transaction on Mobile Computing. He will serve as the Editor-in-Chief for the IEEE Signal Processing Letters from January 1, 2009 to December 31, 2011.