International Journal of Internet, Broadcasting and Communication Vol.7 No.2 56-64 (2015)
http://dx.doi.org/10.7236/IJIBC.2015.7.2.56

IJIBC 15-2-8

A Study on UCC and Information Security for Personal Image Contents Based on CCTV-UCC Interconnected with Smart-phone and Mobile Web

Seongsoo Cho[1] and Soowook Lee*

[1]*Institute of Information Science and Engineering Research, Mokpo National University, 534-729, South Korea*
css66@mokpo.ac.kr
**Kwangwoon Institute for Advanced Study, Kwangwoon University, 26 Kwangwoon–gil, Nowon-gu, Seoul, 139-701, Korea*
wook@kw.ac.kr

Abstract

The personal image information compiled through closed-circuit television (CCTV) will be open to the internet with the technology such as Long-Tail, Mash-Up, Collective Intelligence, Tagging, Open Application Programming Interface (Open-API), Syndication, Podcasting and Asynchronous JavaScript and XML (AJAX). The movie User Created Contents (UCC) connected to the internet with the skill of web 2.0 has the effects of abuse and threat without precedent. The purpose of this research is to develop the institutional and technological method to reduce these effects. As a result of this research, in terms of technology this paper suggests Privacy Zone Masking, IP Filtering, Intrusion-detection System (IDS), Secure Sockets Layer (SSL), public key infrastructure (PKI), Hash and PDF Socket. While in terms of management this paper suggests Privacy Commons and Privacy Zone. Based on CCTV-UCC linked to the above network, the research regarding personal image information security is expected to aid in realizing insight and practical personal image information as a specific device in the following research.

Keywords: *Open-API, User Created Contents, public key infrastructure, User Filtering Contents, Local Area Network.*

1. Introduction

The ubiquitous network technology develops in different forms in the real-world and in the internet. This is due to materialistically differences in technology between the real-world and internet. The internet is relatively easy to realize a business model or an ideology. On the other hand, in the real-world, there is a need to overcome the physical construction expenses and the technical realization. Hence, the cyberspace quickly and easily implements business models and introduces the latest technology, the trend adaptation and

Manuscript Received: Jun. 15, 2015 / Revised: Jul. 10, 2015 / Accepted: Jul. 25, 2015
Corresponding Author: wook@kw.ac.kr
Tel: +82-2-940-5649, Fax: +82-2-916-4751
Kwangwoon Institute for Advanced Study, Kwangwoon University

invigoration, like the web 2.0 and etc are easy. As the current mobile based smart-phone has been getting the spotlight ubiquitous network has developed to the level where it can connect among individual's nodes. The cyber-world technology has materialized in the real world and made a new or the third world. Thus, with the materialization of the internet technology, business model, trend and ideology it strengthens our competitiveness. In other words, taking in to consideration the possible technologies on the internet is an important indicator of the predictable future. The internet is established through the web 2.0 technology, philosopher's participations, idea sharing, and openness combined with XML, Open Application Programming Interface (Open-API), mash-up technology. Especially with the advent of i-phone and google-phone with its mobility will project constantly moving individual simultaneous access to the mobile web. By interlocking the web with the widget and App. which is in charge of processing the location information we are able to utilize more sophisticated customized information based on the smart phone using GPS. With this a semantic web, feasible to infer and predict, is introduced and the smart-phone interlinked with the camera module allows a new pragmatic display service. Here, semantic web means an intelligence technology where the computer understands the actor's intention and can make logical inferences. In the semantic web, the ontology technology transfers the context into the computer friendly language and based on this it streams through the information. In addition, Web 2.0 is the technology that higher the added values through the advance technology – mash-up, collective intelligence, Really Simple Syndication (RSS), track-back, syndication, Open-API – commuting the investigated information of the user implication. These technologies evolve into realizable form through the platform service. Here we need to apply the concept of web as platform. However there are many concerns with the advocacy and increase of cases of adverse effects. Therefore, a User Created Contents (UCC) era met without preparation will meet its limitation. This research seeks to focus on the study of the UCC individual video information security based on CCTV. I would like to discuss about the emerging issues and in importance of information security. Especially I would like to evaluate the systematic method and the technical aspects to protect individual videos. The newly introduced CCTV's treats and individual information security plan will help future researches.

2. UCC Personal Image Information

2.1 Understanding Personal Image Information

2.1.1 Complex Image Information

Image information is limited to media made into videos. But rather than the existing pure information processed forms will increase. This is due to the technological development of web 2.0 the informational retrieval based on meta data, mash-up service through Open-API, inference through Semantic web, and the increase of syndication contents we input additional information. We can categorize to deal with UCC forms as follows.

Table 1. UCC categorized by medium [1]

Category	Subdivision	Acronym	Korea Service Cases
Medium	Text	UCC	Knowledge iN(naver), OhMyNews
	Audio	UCC	personally made coloring
	Image	UCC	josammosa, solobuda, ilryngta, a rambling criticism of chosun news

	Video	UCC	cookjijum dance, adbong eleven, return of ann	
	Packaged	UPC	video+text mete-data+image meta-data+tag complex contents	
Form	Generated	UGC	A	Purely 'A's creativity
	Modified	UMC	A+a= A'	Added idea 'a' of the user based on the original content 'A' A' and A has the same production intention
	Recreated	URC	A+B =C	By combining two different contents 'A' and 'B' and creating a new content 'C'. Yet the production intention was different with that of 'A' and 'B'
	Filtered	UFC	A+B +...+ a+b.. .=C	Adding the user's idea or original content and idea on the original content. This process is done repetitively and the content is transformed into not an individual's idea but take on the characteristic of a group.

UCC can be categorized by its produced method; UGC, pure creativity and User Modified Contents (UMC), User Recreated Contents (URC), User Filtering Contents (UFC), copied materials. Hence, UCC becomes one of a User Generated Contents (UGC), UMC, URC, or a UFC. If we divide UCC by media, we can divide it into two; one with audio and visuals and the other with texts, images, audios and visuals combined together. The latter one is usually used in a different term as User Packaged Contents (UPC). In case of UPC visuals contain, the main contents and the audio, text tags are subordinates. Thus, we mainly focus on the visual information contained in the UGC, UMC, URC, UFC. Especially, in the case of UPC visual is the main content.

2.1.2 Personal Information and Related Law

Personal information, that is, information about live individual, is all information that can be used to distinguish individuals. Information that can be used to recognize individual is broadly divided into two parts. The first is biological information such as gender, height, weight, blood type, and fingerprint, form of iris, Deoxyribonucleic Acid (DNA), and health condition. The second is social information that certifies social relationships such as date of birth, marriage, sexual preference, criminal record, education, religion, and record of participation in political organization. Providing and allowing the use of certain public service of money by making an institutional identification to an individual is also part of personal information.

For instance, there are some records of country such as livelihood welfare recipients, medical protection recipients, insurance certificate for prostitutes, medical insurance certificates, and social security number. Personal information is all that can identify a particular individual by combining it with other information easily even when the particular individual cannot be known. The identification means the information that can be recognized by connecting with other information. Therefore, except for the above peculiar identification numbers such as social security number, driver's license number, real name, and medical insurance number, all information which is able to be combined with other information to identify particular individual is considered as personal information.

The legislation on personal information protection in South Korea is being operated in two separate parts - the public division and the private division. The public division is governed by the acts on personal information protection of private sector. As the relevant individual acts, the electronic government act, special law related to the information disclosure in educational institutions, the social security act, and civil

petitions treatment act are existed. Unlike the public side, there is no law with the feature of basic law on personal information protection in the private division. However, law on promoting the use of information network and information protection] observes the overall matters on the personal information protection. As the relevant laws, the use and protection of credit card information act, information and telecommunication infrastructure protection act, and medical act are existed [2].

In May of 2007, the bill on protection of personal information of public organization was revised and legal base for installation and operation of network camera was made. In other words, personal image information will be conveyed through the internet network by CCTVs connected to the internet, but there is no specific bill or counter move for the protection for it. The network camera in this context is a device that can receive or save the instant image of steady or moving objects and sound and voice that follows it though internet network from a remote area, real-time. Violation of personal information of image information is estimated to increase due to the high definition image filming device.

3. Issues on Information Protection of CCTV

3.1 CCTV and Network

3.1.1 CCTV Linkable to Network

CCTV is a visual supervising engineering machine which conveys image information to a specific user for a specific purpose[3]. Supervision here means observing the change of action while waiting on someone. The domain of CCTV is not only in the Local Area Network (LAN), but with the help of the internet, it expands to Wide Area Network (WAN). That means that CCTV can be operated in remote areas as well.[4] Moreover, by using the web camera, internet makes forwarding and multi-casting of supervising images real-time possible all over the world. Furthermore, specific regions can be observed using the satellite. Such technology is elaborated to ubiquitous sensing network along with the development of geographical map system. 'Google Earth' of Google cooperation is an example. This program has a function that could zoom in to any area in the world. Also anyone can bring the Google map from the Open API environment and upload contents using mash-up technology. If CCTV UCC including the altitude, latitude, and time information is added to the Google map, the infringement of personal information is estimated to be more severe. The image information gathered through the CCTV will seriously threat personal information with the assumption and estimate of mash-up and semantic web technology and various contents.

3.1.2 Technology Associated with CCTV and Iits Status

CCTV is being transferred from closing to openness. CCTVs are changing to opened-style from closed-style. That is, the number of cameras that are linked to network is increasing [5]. The development of computer software especially stimulates the development of bio-recognition technology. Everyone captured by the digital camera will be able to verify one's identity as one's own identifier. A physical trait (finger print, iris, cornea, voice) becomes one's own identifier which makes it possible to verify one's identity. The biological information collected in such way is safer than the validation method using personal passwords. However, it causes various drawback and infringement of personal information by error rates such as FRR(False Refection Rate) and FAR(False Accept Rate).

In South Korea, there are 7 CCTV in 7 metropolitan cities and 466 in local police departments, operating for the use of researching the traffic flow and, up-to-date CCTVs that revolves 360degree from side to side and up to 60-180degree up–and-down are being installed. In addition, there are 712 CCTVs in local police

department in 7 metropolitan cities to regulate traffic violation and also those to regulate parking violation are utilized.

There is no police department using manner CCTV, but it is ran by each local government and private enterprise. The CCTV set up in the Gangnam District Office, which has been a problem, has a zoom function that makes face recognition possible, and the resource is preserved for 3 years. Also, it can turn 180 degree and is able to distinguish human faces from the distance up to 500 meters.

Moreover CCTV to find vehicles in want and other various applied CCTV are being introduced for convenience of administration and prevention of crime, but it is in blind stop of personal information violation because of lack of related law, technological security measurements, and professional manpower in many cases. In the private sector, especially, there are CCTVs with zoom-in function that can clearly recognize people to 500 meters away, revolve 360 degree, and recording which are not included in the statistics. To minimize such problems, technical security measurements has to be set through agreement and consent on the subdivided standard and sensitivity of privacy of the agent that installs the CCTV and various groups that are in connection of interest with such agent.

3.2 CCTV and Information Security Issue

3.2.1 Hidden Cameras and Information Security Issue

Pornographic is a difficult idea to define. In the States the miller tests suggests a standard to define pornographic. If we look at the standards; first the jury decides whether the piece is acceptable to an average person's regional moral standards. Second, whether the piece is violating the state's law and is portrayed in a patently offensive method. Third, whether the piece lacks literary, artistic, political, or scientifically values If we apply these standards to the video UCC's we can distinguish obscene contents to a certain level but not totally [6]. In the new coming technology environment the largest violation in personal video information would probably come from small CCTV. Especially, foreign video platforms and video platforms that lack safety device to protect the children and teenagers have serious problems. In July, 2003 the Korean Supreme court made a judgment that linking porn sites to internet web pages can receive a criminal penalty. But the UCC is left in the holes. Theses pornographies made through hidden cameras are introduced on porn sites under the name of UCC.

3.2.2 CCTV and Network Camera Issues

The network camera has the following problems as compared to the CCTVs network camera. First, it becomes the method of the spread of the video information. Once the video information is spread on the internet due to hacking or the negligence of the manager it is impossible to withdraw. Second, it is difficult to figure the responsibility due to the expansion of the details and range of the spill. Close-CCTV has limited number of people who have access to it. But open-CCTV is open to the internet users online. It is not easy to figure out whether the spill first occurred from the inside person or from a hacker or whether it was due to the carelessness. In addition, once the material is distributed (messenger, P2P, E-mail, bulletin board and etc) among many people the responsibility and degree of penalty becomes very difficult to measure. Third, people become passive with the consciousness indwelled that they are always being monitored. If we are grown under the CCTV surveillance unconsciously from our very youth we will bring about a Big-brother system. Passive people kept under observation lives under a Panopticon, where their freedom to express and freedom of privacy is violated, accept it as a natural thing. The Panopticon is a type of prison building designed by English philosopher and social theorist Jeremy Bentham in 1785. The concept of the design is to allow an observer to observe (-opticon) all (pan-) prisoners without the incarcerated being able to tell

whether they are being watched, thereby conveying what one architect has called the "sentiment of an invisible omniscience [7]. Fourth, CCTV is edited and combined with others by internet users and the edited version is posted on the web. In this case, it has a risk of the first intention of the CCTV becoming different from that of the beginning. But with the advancement in individual's computer and editing software and the extraction skills, even with the limited members we cannot say we will be completely free from the CCTV information being used in UCCs. Fifth, vocal, text, tag will be included in the information. You can add the location of the CCTV and the recorded time. In addition to this when texts and tags are added CCTV will become a tool that will candidly show ones personal information. The video containing diverse information becomes a dangerous tool infringing others rights. Sixth, it is a violation to one's own right of information discretion. Personal information should be up to the person to produce, transfer, remove, and recycle. This is called individual right to control the circulation of information relating to oneself.

But, there is no way to avoid the CCTVs installed in public places. The only way to avoid it would be to not go on the streets or to cover your body and face so that no one would be able to recognize you [8]. Eventually the collected information from CCTV becomes an inevitable environment. Recently CCTV has developed a movement recognition automatic focus and information collective device so there is no way an individual can avoid being shot by the CCTV.

4. Information Security Plan of CCTV

4.1 Technological Methods of Protection

Technological methods can be broadly divided into physical spaces and cyberspaces. First, there is security plans in the physical spaces at the stage of collecting visual information through the CCTV. Privacy Zone Masking is a technique which makes certain parts invisible among recorded screen using some techniques such as blurring some parts of screen or masking techniques according to installation and running angle of image information processing devices when it invades privacy. Recently installed CCTVs in major buildings are cameras which have the Pan/Tilt/Zoom (PTZ) function. The control of PTZ is consisted with zoom which drives lens, motor, tilt and pan motor. Above all, CCTV's major filming control is done by moving the tilt, pan and motor to the target quickly, quietly, smoothly and precisely to the target. This is developed as more advanced and standardized optional services are required. The representative advanced functions of CCTV are pre-set, pattern, group, swing, privacy zone masking, auto flip, motion tracking, auto parking and schedule [9]. Lately commercialized CCTV includes privacy zone masking skill but it is a selective function for users, not an obligation. Especially it, however, is problematic that it does not have functions which can save, change or trace privacy zone masking skill's history of use based on time. We can develop a monitoring device into software through long distance managed CCTV servers or short distanced control rooms. Instead of privacy zone masking technique, there are some techniques that restrict using software or give limitation to the zoom function and CCTV's resolution. More precisely, it is removing support of zoom function to make it undistinguished as enlarging some parts such as faces or installation of products having lower resolution which cannot collect image information except for the original purpose.

Second, there is security during the transferring and utilizing process of the visual image. It is mainly protection in cyberspace. More specifically, the prevention of hacking through IP filtering and IDS when CCTV is connected to the internet could be an example. In particular, SSL is very efficient in CCTV linkages circumstance because it is layers of coded networks so it can be utilized in not only Hypertext Transfer Protocol (HTTP) but also Network News Transfer Protocol (NNTP) and File Transfer Protocol (FTP). Basically SSL guarantees authentication, encryption and integrity. In addition, PKI for authentic

techniques or Hash function skills can be applied to it [10]. Also, designing complicated security system is possible through PKI. In other words, it confirms users with digital authentication and codes transmission and reception data by using public key consisted by codes and decryption key. This is a developed system for securing creditability and security of e-commerce or information circulation and it has secrecy function, the function of identification of references and confirmation of changes from information. Also, it is possible to track when image information is leaked because it can identify the user's references by tracking the image information with PKI. Furthermore, there is another method which gives technical protective coat to image information as confining uploads of other information. Also, it is possible to develop techniques to simply see the image information and prohibit cutting or editing like PDF files.

4.2 Management Security Plan

4.2.1 Privacy Commons Plan

UCC is a creativity that contains the creator's personal experience. The problem is with the current personal visual equipment distribution and the advancement of web 2.0 UCC is emerging as one of the main contents in companies and governmental bodies. But it is impossible to regulate UCC that is different in quality and quantity than ones that the previous media contents produced. We would need to protect this on the basis of information privacy. Hence, the main actor should know about the changes, transfers, deletes of the related information and should be the one who supervises it. In order to protect this, the main actor should be the one who decides the degree of preservation of the UCC when one distributes it. A more specific scenario would be the following cases. When the UCC producer uploads the UCC, he sets the degree of privacy. The setting up should be an easy and simply process. For example, access permitted when logged into this web. This will prevent people from taking and transferring the information. Access allowed to only specific people. This allows the person to make the decision to which he will permit the access to his privacy. This means that if a person who was not allowed to see, he will be held responsible for invading one's privacy regarding the reference, distribution etc. This kind of privacy set up can be done by a simple tag like a mark. Privacy commons is expected to bring out the following outcomes. First, it gives a method to have self-control over UCC which is very difficult to control by the governmental administrative. Second, the administrative can have direct control over the platform and portal business, where UCC is mainly produced, spread and distributed, along with emphasizing the currently existing portal's responsibility.

4.2.2 Designating a Privacy Zone

Currently CCTV is being installed not just for public reasons but also for private reason, but due to the lack of regulations, there is a blind spot for privacy. Especially the risk of people turning passive with the unconsciousness that they are being watched everywhere all the time, should be minimized. In order to prevent this social phenomenon, the governmental institutions and civic groups must establish a privacy zone. The established privacy zone must secure ones privacy based on the individual's choice. In other words, we must establish privacy zone in order to protect people's privacy in the physical world. We have some examples to use the privacy zone. First, a road above the certain level (i. e. wideness over 5-10 meters of the sidewalk), the 1-2 meters of the sidewalk can be decided as a privacy zone. The privacy zone should not fall within the filming angle of the CCTV. There also should be hardware equipments installed that could protect privacy depending on the road condition. Second, in cases, where the road is narrow, we need to investigate if there is a detour route that could secure one's privacy. People would need to have an alternative route to avoid a big brother society. Especially there is a need to have restricted CCTV filming regulation based upon the crime occurrence time, place and frequency. We would need to announce the time that is being filmed.

Third, certain private companies could have space that secures ones privacies like café, hotel lobbies and also companies that acknowledges privacies can mark the privacy zone from the entrance to the café and make a publicized private area. Fourth, there should be a privacy zone other than the road where people can fully enjoy their law of secret communication. For example, we need to establish a zone in the public area where people will have privacy in communication and expression and be intervened neither by authority nor by any satellite or google shooting whether legal or not. This expects to have the following effects. First, the privacy zone itself will have a symbolic meaning that the governmental body actively works to secure the people's privacy. Second, it will activate the current lagged privacy security industry and the research on privacy security will bring about advancement in blocking hacking and thus enhance the information security industry. Third, it will reduce the potentially ambiguous zone of privacy that the law not able to cover due to the fast paced developing technology environment. In other words, it could be understood that even with the advent of any kind of future technology, the privacy zone that an individual has selected cannot be intervened. Fourth, on the sidewalks, to give their right to the people to choose if they walk a CCTV filmed area, they can find a place within a five to ten minute walk where there is no CCTV. This would be to relieve the people's discontent because of the constant surveillance and filming and allow them to pursue their happiness and information right and information privacy in a physical area.

5. Conclusion

In a ubiquitous environment, the physical and cyberspace is naturally connected and realized the reinforced reality, sensing network, situation recognition system and so on. Then, the CCTV connecting to the internet and becoming an open network camera system are becoming natural phenomena in the technological development process. But the distinguishable personal information put into the video becomes a meta-information or becomes mash-up with the existing contents on the internet. In addition an individual's longitude, latitude, time, video information, tag, vocal information becomes a distinguishable source like the social security number and if this becomes predictable and inferable through the semantic web technology soon, there will be no privacy. In order to reduce this risk to the minimum, we looked at the personal video information related issues brought up by the CCTV and sought the solution in a technical and management way. The first technical solution includes the privacy zone masking skill or limiting the resolution and zoom to the publically used CCTV in the physical space. The second includes the use of the security technologies as is IP filtering, IDS, SSL, PKI, Hash in the process of the video information transfer and utilization in the cyberspace. The effectiveness of the technical security is enhanced when it is used along with management security. In the case of management, the first proposed method is to make CCTV an alternative for security in the public sector. For instance, we should install a CCTV for the purpose of the governmental institution to collect materials in order to prevent crimes, collect evidences secure facility and prevent fire, restrict entrance a place to for the individuals to procure their information privacy simultaneously and give individuals the right to permit or reject the government to collect their visual information. This is the called a privacy zone; a designated place where one's privacy is secured. The second proposed method is to give a right for deciding owns information to the private sector for the CCTV security. For example, when one uploads one's UCC on their blog, homepage, or youtube (www.youtube.com), portal sites, they can choose the sharing boundary. This is called 'privacy commons'. It has been proven through the creative commons movement in the copyright section that privacy has been respected. As we have seen above studies of personal video information security based on CCTV-UCC interlinked with the network gives an insight and helps realize a practical and specific information security for future studies.

Acknowledgement

The present Research has been conducted by the Research Grant of Kwangwoon University in 2014.

References

[1] Jang-Mook Kang, *UCC butterfly and Ubiquitous typhoon*, CommunicationBooks Publication, South Korea, 2008.
[2] Minho Kim. "A problem and overview for public law on information privacy," *TOJI, A Public Law Review*, Vol. 37, pp. 1-209, 2007.
[3] Min Ho Kim, "A Study on the Current Issues about the Personal Information Protection Act in Korea," *Korean Public Land Law Association*, Vol. 37, No. 1, pp. 209-224, 2007.
[4] Korea Communications Commission, CCTV Guideline for information privacy, 2006.
[5] Jang-Mook Kang, "A study for electronic observation in argument reality environment (RFID, CCTV). Korea digital contents Society," *Journal for Korea digital contents*, Vol. 7, No. 2, pp. 75-82, 2006.
[6] Francisco R. Klauser, "Difficulties in revitalizing public space by CCTV-Street prostitution surveillance in the Swiss city of Olten," *European Urban and Regional Studies*, Vol. 14, No. 4, pp. 337-348, October 2007.
[7] Lang Silke Berit, *The Impact of Video Systems on Architecture*. *Dissertation*, Swiss Federal Institute of Technology, 2004. http://en.wikipedia.org/wiki/Panopticon(sited 2010. 12.)
[8] Jang-Mook Kang, *CyberLaw*, Gilbut Publication, South Korea, 2003.
[9] Ruth Costigan, *Ruth Identification from CCTV: the risk of injustice*, Criminal Law Review, pp. 591- 608, 2007.
[10] Luis M. Fuentesa, Sergio A. Velastin, "People tracking in surveillance applications," *Image and Vision Computing*, Vol. 24, No. 11, pp. 1165-1171, 2006.
DOI: 10.1016/j.imavis.2005.06.006