Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 960416, 9 pages
http://dx.doi.org/10.1155/2015/960416

Research Article

Study on Strengthening Plan of Safety Network CCTV Monitoring by Steganography and User Authentication

Jung-oh Park[1] and Sanggeun Kim[2]

[1]*Department of Information Communications, Dongyang Mirae University, Seoul 152-714, Republic of Korea*
[2]*Division of Computer Engineering, Sungkyul University, Anyang-si 430-742, Republic of Korea*

Correspondence should be addressed to Sanggeun Kim; sgkim@sungkyul.edu

Received 16 October 2014; Accepted 4 December 2014

Academic Editor: Seungmin Rho

Copyright © 2015 J.-o. Park and S. Kim. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Recently, as the utilization of CCTV (closed circuit television) is emerging as an issue, the studies on CCTV are receiving much attention. Accordingly, due to the development of CCTV, CCTV has IP addresses and is connected to network; it is exposed to many threats on the existing web environment. In this paper, steganography is utilized to confirm the Data Masquerading and Data Modification and, in addition, to strengthen the security; the user information is protected based on PKI (public key infrastructure), SN (serial number), and *R value* (random number) attributed at the time of login and the user authentication protocol to block nonauthorized access of malicious user in network CCTV environment was proposed. This paper should be appropriate for utilization of user infringement-related CCTV where user information protection-related technology is not applied for CCTV in the future.

1. Introduction

Due to networking of CCTV and openness of the internet, the necessity to protect privacy video data and information safety, trust, protection, and concealment is in demand, and as the according application technique, the study on steganography method which inserts confidential information to the transfer media is actively in progress.

The existing web has much vulnerability, and as CCTV was involved with networking, it became a problem that CCTV is exposed to such vulnerability of web. Also, CCTV videos are related to privacy, and if such videos are exposed to unspecified public, it would be a sufficiently sensitive issue.

Recently, there are many problems related to CCTV; the manager does not frequently change the public IP or dynamic IP of network camera, rendering it easy to be exposed outside, and once IP address is leaked, the crack program breaking the password is used to access the administrator account and have the monitoring video leaked at any time. Network monitoring camera, however, has a large data size and sends data through streaming unlike other IT resources; thus it is hard to change the IP address and is easily exposed outside. Due to such issues, it is only a matter of time for the monitoring video to be leaked. Other than that, there is possibility of leakage of CCTV videos due to several threats, and data security must be provided accordingly. Existing studies [1–17] on CCTV security concentrated on security structure of CCTV network infrastructure, security policy, and utilization under specific environment (crime prevention, etc.). This paper shifts from such general topics to propose a user authentication protocol under network CCTV environment which reinforces CCTV monitoring with steganography and prevents malicious user access. International trends of CCTV security are given in Table 1.

2. Related Studies

2.1. Network CCTV System. By inserting IP to the existing CCTV, CCTV can be managed individually, and as long as internet is available, remote management and remote monitoring are available. Such network CCTV system is as in Figure 1.

Table 1: International trends of CCTV security (purpose and characteristics).

Country	Purpose	Location	Characteristics
Korea	Theft prevention, traffic and parking, and disaster prevention	All regions of Korea	Operating integrated CCTV control centers by local governments around the nation
UK	Theft prevention and prevention of riot, protest, and terrorism	All regions of UK	Converted from analog to HD CCTV, installing large number of CCTV compared to population
Germany	Building security such as alert on theft, fire, intrusion, and robbery	Major buildings	Video equipment related to theft and intrusion combined as one
UAE	Prevention of terrorism and various crimes	Facilities such as schools, hospitals, and parks	Entirely relies on importation with high ratio of CCTV used to prevent auto theft
United States	Public security such as homeland security and disaster prevention	All regions of the United States	Has largest market size and quickly applies latest technological trends (intelligent CCTV)
Switzerland	Homeland security, public security, and corporations	Major public institutions	High ratio of CCTV used to maintain public order
China	Crime prevention and public security	Major public institutions, automobiles, and households	Low ratio of HD CCTV and low availability

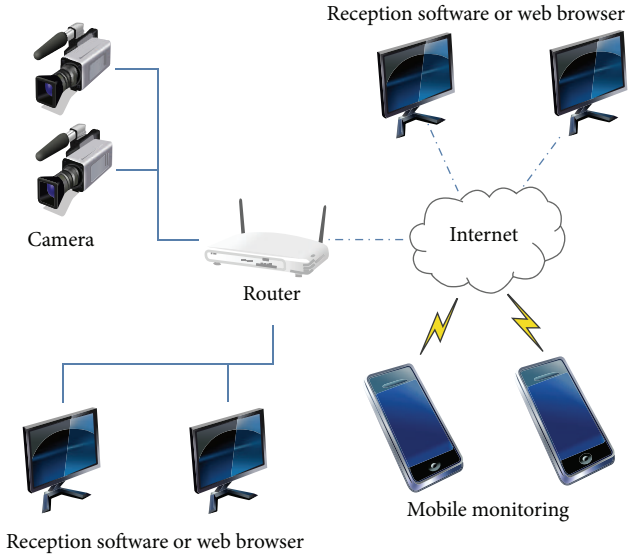


Figure 1: Network CCTV system.

2.2. Problems of Network CCTV Systems. As CCTV gets involved with networking, there are many emerging issues. The number of police protecting the safety of the citizens is increasing every year, but due to the increase in social violent crime occurrences and public order issues, the installation/operation of network-based CCTV systems are expanding nationwide for the purpose of citizen protection and personal security. Particularly, thanks to the advancement of internet technologies, the utilization scope became more diverse from illegal trash dumping to public order/crime prevention to illegal parking/stop, and so forth.

On the other hand, despite the expansion of installation/expansion of CCTV system, relative absence of clear governmental guidelines and reckless introduction with standards are emerging as security issues [18, 19].

The purpose of CCTV in different nations is prevention of major crimes and promotion of public security. Existing analog CCTV devices are changing into network-based digital CCTV with HD screen. The market for network-based CCTV system is growing for operation of integrated control centers. Examples [20–22] of security scenarios that can occur in network-based CCTV systems are as follows.

① Collection of information by CCTV system that uses public IP: as the system is linked to various paths, exposure of IP address as problem that information on the operating system and application used by CCTV system server can be collected with ease.

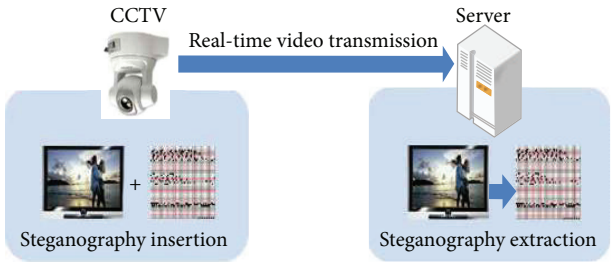


Figure 2: Overall structural diagram.

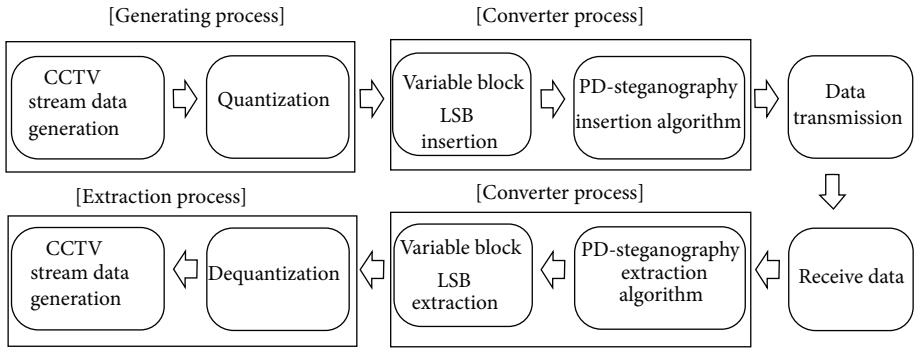


Figure 3: Overall data flowchart.

Hackers can use this as a starting point to make different hacking attempts based on information collected from each server.

② Sniffing and spoofing of sections with security vulnerabilities: since all IP-based CCTV systems communicate via different network devices and servers in a public network, information can be exposed when a section without security infrastructure is hacked.

③ Lack of data safety from nonapplication of encryption on video data: existing analog CCTV and network CDTV with relatively low hardware specifications have a problem in which real-time data cannot be encrypted. This results in easy exposure of data stored in servers.

④ Security vulnerabilities of CCTV control centers: as control centers are always connected to network because they need to manage and control CCTV on a real-time basis, security vulnerabilities of server and control PC can expose ID and password of important administrator accounts. Hacked CCTV systems can be used as a means to attack internal infrastructure and attack route.

As shown in the hacking scenarios described above, hacking of important information and exposure of CCTV information have reached a dangerous level of security alert for network CCTV systems resulting in leakage of confidential information of public institutions and corporations, deletion or alteration of important information such as major theft crimes, and unauthorized release of private CCTV information.

3. Video Steganography Application Plan for Network CCTV Monitoring Security

As in Figure 2, the overall system structure diagram shows that when sending the video from the CCTV, the steganography is inserted realtime before being sent to the server, and then the server extracts the steganography from the video again.

This report proposes a method to protect the system by inserting steganography to the real-time video of CCTV monitoring system provided in open source. Figure 3 is the overall data flowchart of this report. This structure is in three different work processes of generation, conversion, and extraction. The generation part generates the video data from CCTV and converts the video data into bits. The conversion part is the LSB process for the bit-converted video data and proposed steganography insertion application. The extraction part is the process of reverse-quantization of data extract by LSB method and generating video data. The proposed steganography input method is as in Figure 4.

Figure 5 shows the application of shift to the corresponding data line by the same rule as in Table 2. For example, the data in Figure 4 shall have the time value of image filmed with CCTV, user name, key value of CCTV, and so forth.

4. User Authentication Protocol to Block Malicious User

Figure 6 is the overall outline diagram of the proposed protocol. In the proposed user registration process, along with the user authentication, the user and related CCTV are

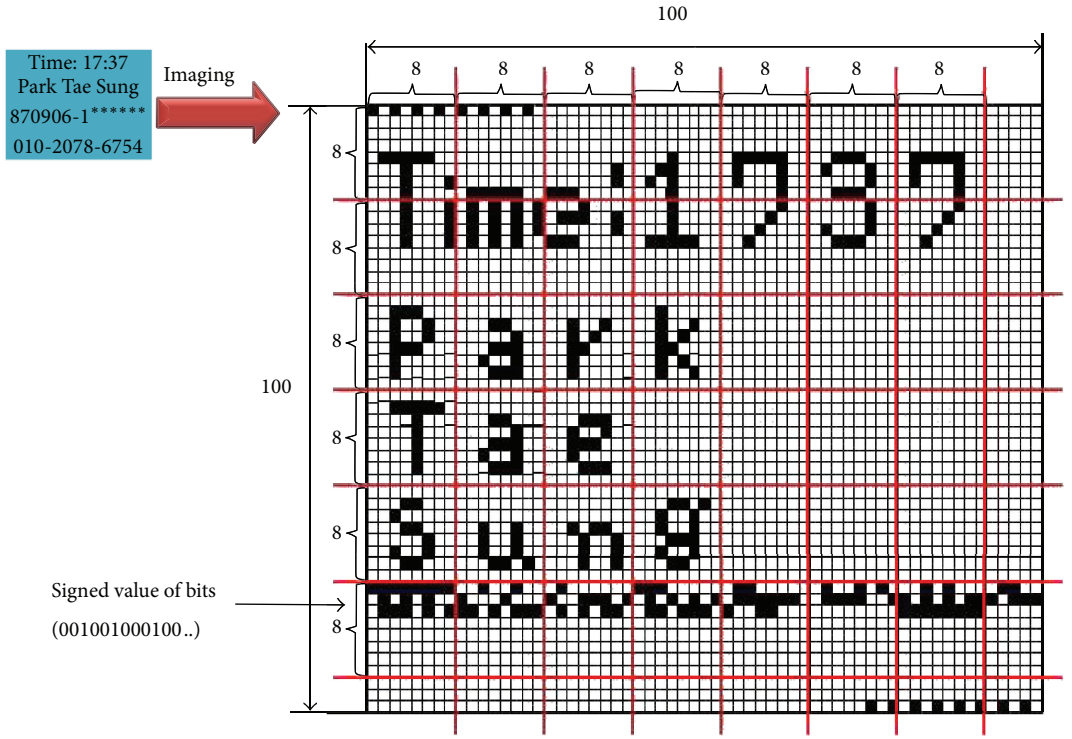


Figure 4: After shift of steganography-inserted data.

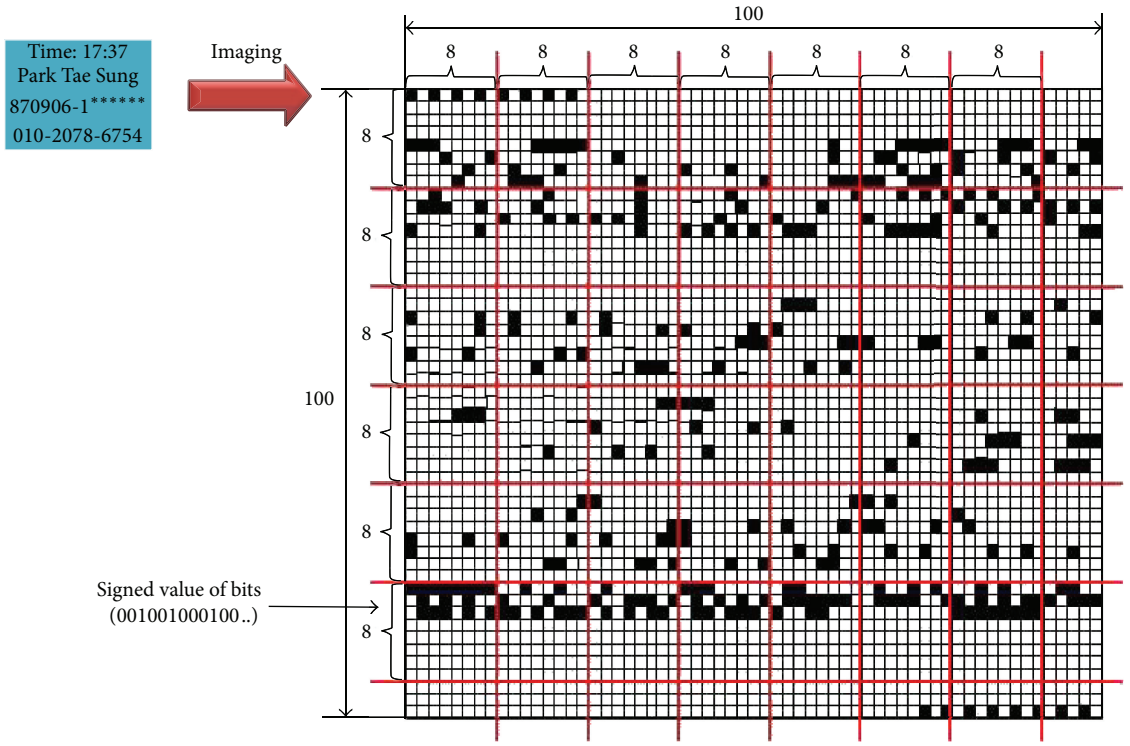


Figure 5: Before shift of steganography-inserted data.

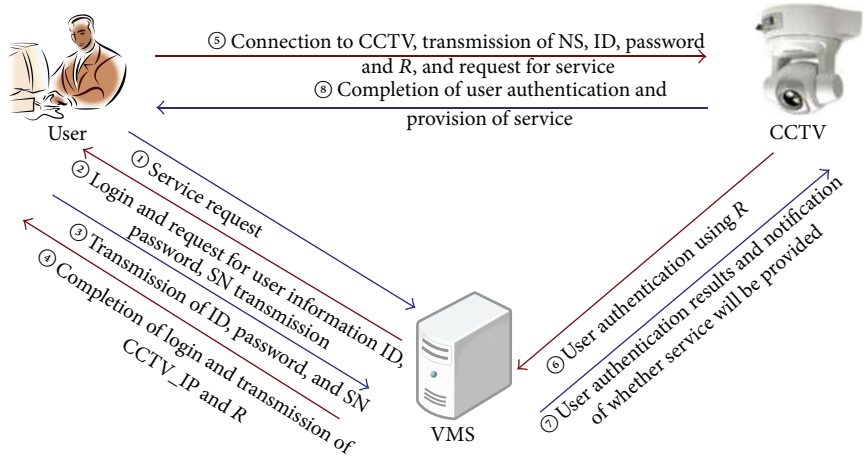


Figure 6: Overall composition diagram.

Table 2: Steganography data shift rules.

Line	Shift
1	None
2	$\gg 1$
3	$\gg 3$
4	$\gg 6$
5	$\gg 10$
⋮	⋮
n	$\gg n(n-1)/2$

synchronized at the same time providing the SN of CCTV, and in user authentication process, this SN and random number attributed to the user are used to strengthen identity authentication, and it is rendered impossible to leak CCTV video by password unlock crack or simple CCTV IP access.

4.1. User Registration Protocol. Figure 7 is the user registration process of the proposed protocol. The proposed user registration protocol is achieved by executing the following procedure.

① The user sends the network CCTV video service request message to the operation PC of VMS.

② The operation PC of VMS requests the user information necessary for member subscription.

③ The user requests the user information for member subscription.

Response {User Data(Name, Num)}.

The corresponding information is, respectively, user's name and user's resident registration number.

④ The operation PC of VMS sends the received user information to the identity confirmation agency and requests authentication.

Verify User Data confirm {User(Name, Num)}.

VMS does not feature an agency to identify the information for the user. Therefore, the operation PC of VMS sends the data received from the user to the identity confirmation agency to request the confirmation of the information for the user.

⑤ The identity confirmation agency checks the user's personal information, and if the information is correct, it sends an approval message to the operation PC of VMS, and if not, it sends a rejection message.

⑥ The operation PC of VMS sends the response message received from the identity confirmation agency to the authentication server.

⑦ The operation PC of VMS checks the user information with the received message.

⑧ The authentication server sends the approval message for the user information to the operation PC.

⑨ The operation PC sends the approval message received from the authentication server to the user.

⑩ The user encrypts the ID and password to be used with the public key of VMS and sends it to the operation PC of VMS.

Send $\{E_{VMS_{Pu}}(ID \parallel PW)\}$.

The user sends the ID and password encrypted with the public key of VMS so that the user ID and password can only be decrypted by VMS and it is safe from external attacks such as password speculation attack.

⑪ The operation PC decrypts the data received from the user with the personal key of VMS to extract ID and password.

Transaction $\{D_{VMS_{Pri}}(ID \parallel PW)\}$.

⑫ The operation PC sends the value hashed to prevent the exposure of user's ID and password to the authentication server.

Send $\{ID \parallel h(PW)\}$.

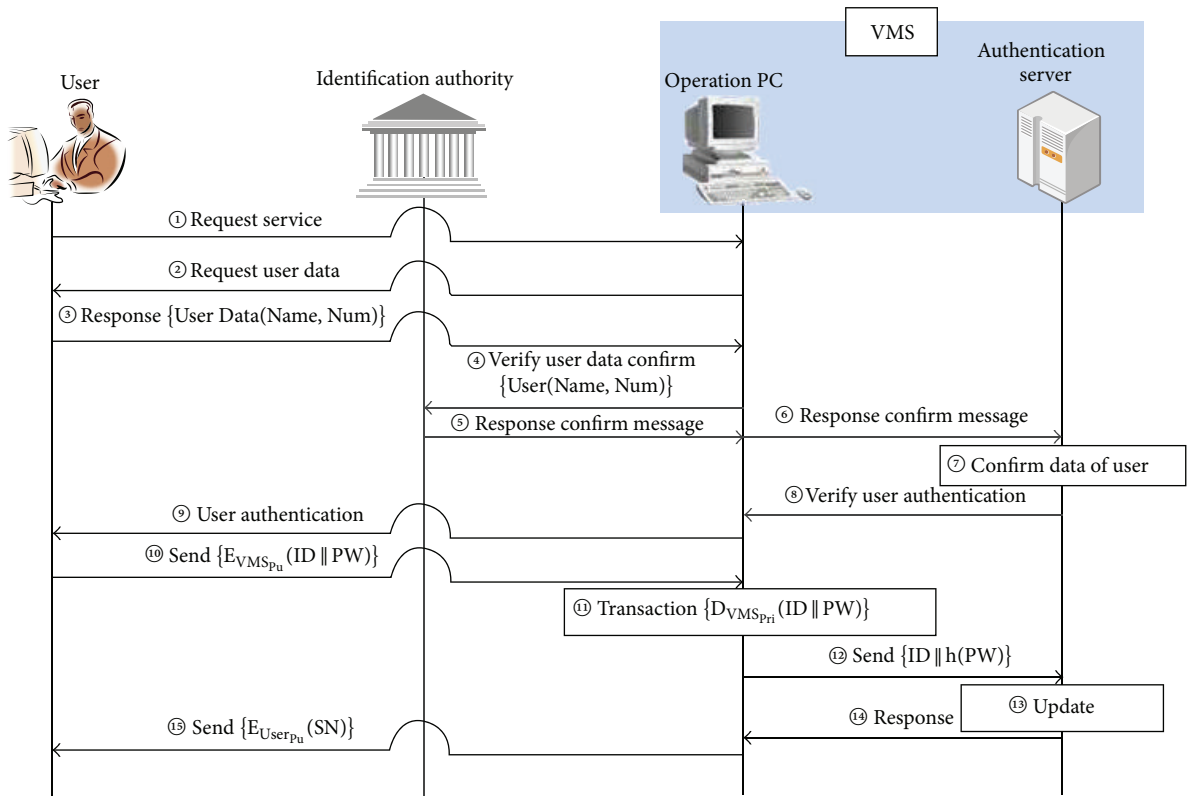


Figure 7: Proposed user registration protocol.

⑬ The authentication server registers the received user information.

⑭ The authentication server sends the result for the completion of member subscription to the operation PC.

⑮ The operation PC encrypts the SN value of CCTV necessary for the authentication process with the public key of the user and sends it.

Send $\{E_{User_{Pu}}(SN)\}$.

The objective of this user registration protocol is to check the user information and obtain SN which is the information needed when requesting service from the network CCTV that the user wants to see.

4.2. User Authentication Protocol. Figure 8 is the proposed user authentication protocol process.

The proposed user authentication protocol is achieved by executing the following procedure.

① The user makes a service request to the operation PC of VMS.

② The operation PC checks the member subscription of the user before providing the service, and if the user is a member, it requests the user information and CCTV SN distributed at the time of member subscription.

③ After encrypting the hashed data of user ID, password, and CCTV SN value with the public key of VMS, it is sent to the operation PC.

Response $\{E_{VMS_{Pu}}(ID \parallel PW \parallel h(SN))\}$.

④ The operation PC decrypts the received data with the personal key of VMS to check the SN value of CCTV and hashes to prevent exposure of user ID and password and sends it to the authentication server.

Send $\{ID \parallel h(PW)\}$.

⑤ The authentication server checks the received ID and password and generates a single-use R value for the corresponding user.

⑥ The authentication server sends the generated R value to the operation PC.

⑦ The operation PC encrypts the corresponding port number of IP information of CCTV for the SN value and R value received from the authentication server together with the public key of the user and sends it to the user.

Send $\{E_{User_{Pu}}(R \parallel CCTV\_IP \parallel P\_Num)\}$.

⑧ The user decrypts the received data with the personal key of the user to access CCTV. The user connects the data where SN of CCTV is encrypted with the public key of CCTV to the data where the user ID,

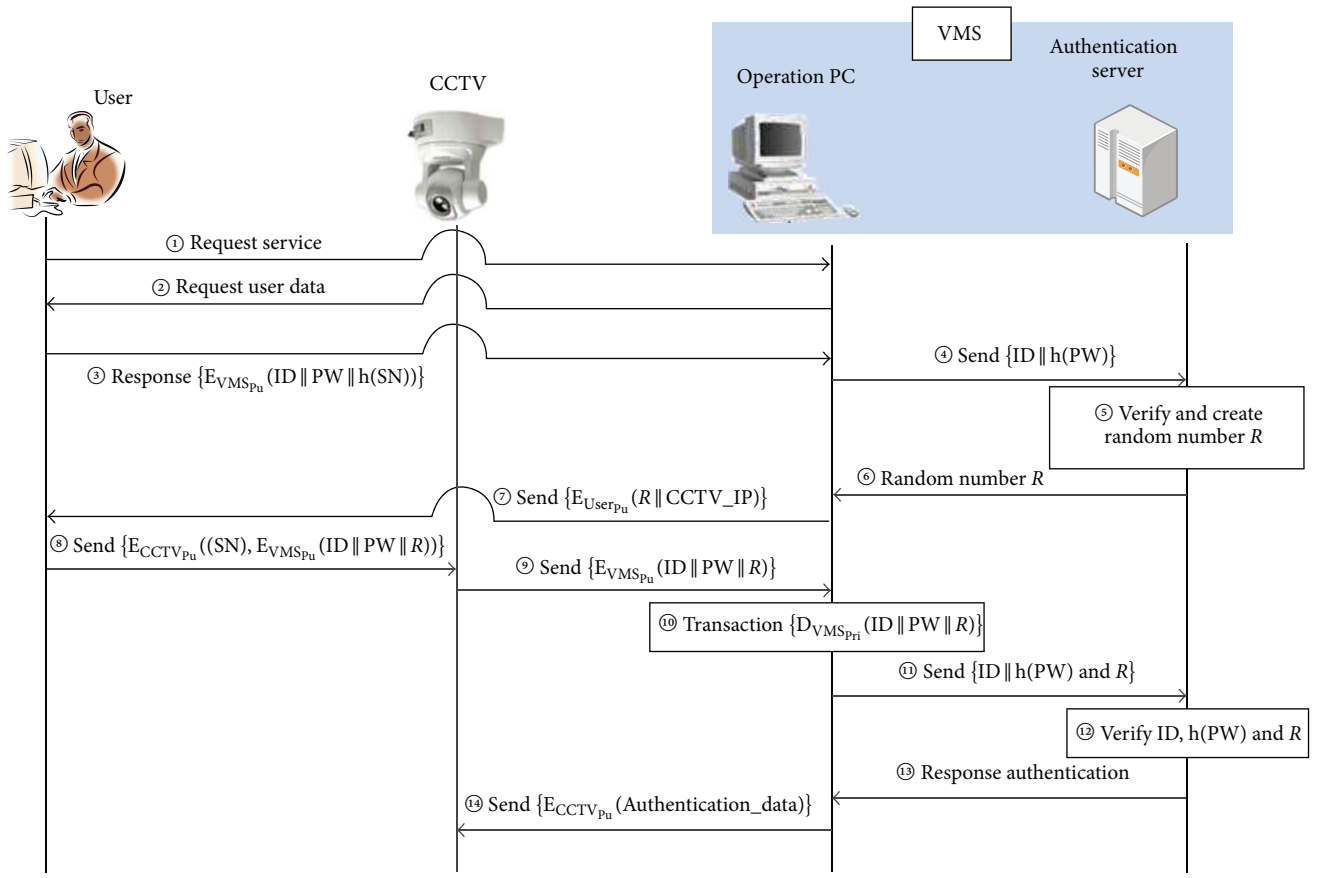


Figure 8: Proposed user authentication protocol.

password, and random number (R) are encrypted with the public key of VMS and sends it to CCTV.

Send $\{E_{CCTV_{Pu}}(SN) \parallel E_{VMS_{Pu}}(ID \parallel PW \parallel R)\}$.

⑨ CCTV decrypts the received data with the personal key of CCTV, and if the SN value matches that of the CCTV itself, it sends the data encrypted with the public key of VMS to VMS.

Send $\{E_{VMS_{Pu}}(ID \parallel PW \parallel R)\}$.

⑩ VMS operation PC decrypts the received data with the personal key of VMS and extracts ID, password, and R value.

Transaction $\{D_{VMS_{Pri}}(ID \parallel PW \parallel R)\}$.

⑪ The operation PC transfers the hash value and random number R to the authentication server in order to prevent exposure of ID and password.

Send $\{ID \parallel h(PW) \parallel R\}$.

⑫ The authentication server verifies that the received ID, password, and R value are the same as those provided by VMS.

Verify ID, h(PW), and R.

⑬ Send user authentication message to the operation PC.

⑭ Operation PC encrypts the user authentication message with the public key of CCTV and sends it to CCTV.

Send $\{E_{CCTV_{Pu}}(Authentication\_data)\}$.

5. Implementation and Performance Evaluation

Figure 9 shows the VMS Client access of the proposed system. It shows the insertion of SN value and R value attributed from the server and the port number, and the server IP is also showing.

The proposed user authentication protocol is used to authenticate the SN acquired by the user when registering the user. In the authentication process, checking SN and comparing information such as R value, ID, and password of the corresponding session render it safe from many threats, and by using the PKI-based encryption mechanism, data confidentiality is guaranteed, and by applying hash algorithm to user's personal information, the personal information is also guaranteed integrity.

Figure 10 shows the photo before and after the insertion of steganography. Through this Figure, it can be shown that there is no visual difference in the video despite the insertion

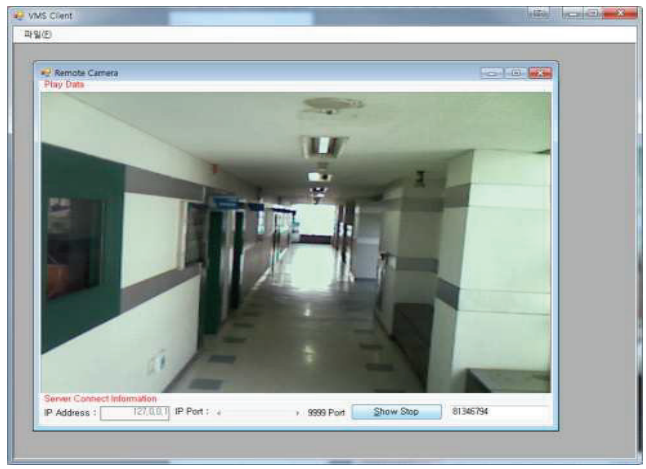
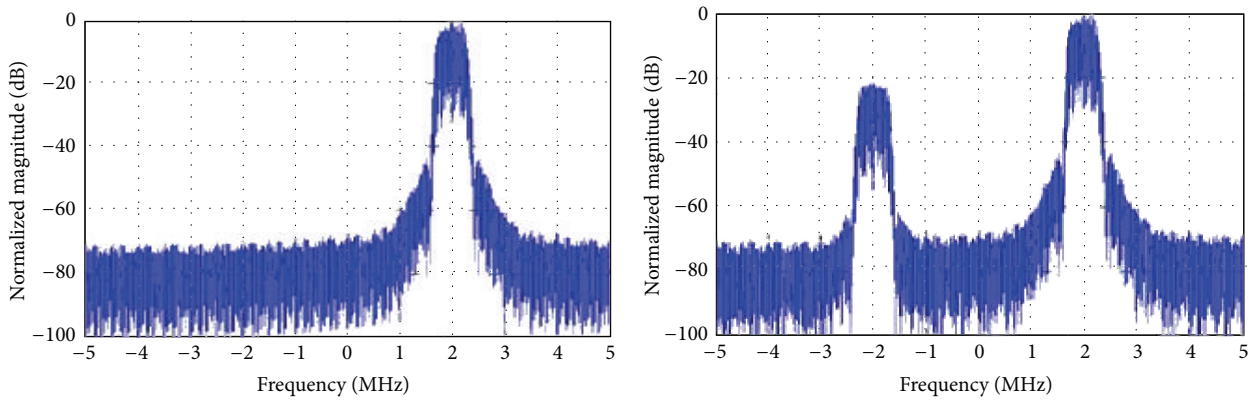


Figure 9: VMS Client implementation.

(a) (b)

Figure 10: Before (a) and after (b) the insertion of steganography.



(a) (b)

Figure 11: Comparison of frequency before (a) and after (b) the insertion of steganography.

of steganography, and through Figure 11, it is shown that the increase of complexity in data leads to the increase in the strength of encryption.

The safety of the existing network CCTV system environment and the proposed system is as in Table 3.

6. Conclusion and Future Research

In this report, the image checking technique through steganography for security of image transfer process and user authentication protocol to block malicious users in network

Table 3: Comparative analysis of safety.

	No authentication	Existing system	Proposed system
Password speculation attack	Weak	Weak	Safe
User impersonation attack	Weak	Weak	Safe
Replay attack	Weak	Weak	Safe
Omnidirectional safety	Weak	Weak	Safe
Website hacking	Weak	Weak	Safe
Input contents falsification, keyboard hacking	Weak	Weak	Safe

CCTV environment was proposed. In future, it would be necessary to continue to complement weakness for greater safety against attacks of malicious users and search for a more efficient algorithm and authentication method.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] S. Kim, *A Study about Ways to Improve Crime Prevention Effects of Crime Prevention CCTV*, Dongguk University, 2007.

[2] H. No, *Effective Use of CCTV for Crime Prevention*, Korean Association of Public Safety and Criminal Justice, 2004.

[3] E. E. Zelniker, "Global abnormal behaviour detection using a network of CCTV cameras," in *Proceedings of the 8th International Workshop on Visual Surveillance*, Marseille, France, October 2008.

[4] S. Baek, *Design and Implementation of a Video Surveillance System in a Wired/Wireless Network Environment*, Dankook University, Yongin, Republic of Korea, 2006.

[5] C. Im, *A Study on the Problems with the Use of CCTV for Crime Prevention and Ways for Improvement*, Yonsei University, 2007.

[6] Y. Shin, "A study on the protection of personal information following the introduction of CCTV at public institutions," *Journal of Korean Association for Regional Information Society*, vol. 11, no. 2, pp. 1–21, 2008.

[7] I. Minhyeok, "The direction of crime prevention policies through analysis of the crime prevention effects of crime prevention CCTV," *Korean Political Science Association*, vol. 12, no. 4, pp. 77–101, 2008.

[8] S. Go, "A study on human rights infringement and likelihood of risks when CCTV video images are stored long term indiscriminately," *Internet Law*, vol. 27, pp. 49–72, 2005.

[9] Y. Kim, *The Current State of Development of IP Cameras, Storage Solutions and Video Analysis*, Korea Educational Center of Future Technology, 2011.

[10] M. Lee, "The current state of CCTV regulations and its implications," *Korea Association for Telecommunications Policies*, vol. 18, no. 12, 2006.

[11] Y. Jo, "Efficient construction of an integrated control environment using an existing disaster briefing room," Regional Information, 2009.

[12] Korea Educational Center of Future Technology, *Business Outlook for Implementation Strategies of Next-Generation Video Surveillance and Intelligent Integrated Security Control Systems*, Korea Educational Center of Future Technology, 2011.

[13] I.-S. Lee and W. S. Yi, "Security requirements for network CCTV," *World Academy of Science, Engineering & Technology*, vol. 70, no. 47, p. 184, 2010.

[14] A. J. Lipton, C. H. Heartwell, N. Haering, and D. Madden, "Automated video protection, monitoring & detection," *IEEE Aerospace and Electronic Systems Magazine*, vol. 18, no. 5, pp. 3–18, 2003.

[15] L. Li, W. Huang, I. Y.-H. Gu, R. Luo, and Q. Tian, "An efficient sequential approach to tracking multiple objects through crowds for real-time intelligent CCTV systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 38, no. 5, pp. 1254–1269, 2008.

[16] N. Buch, S. A. Velastin, and J. Orwell, "A review of computer vision techniques for the analysis of urban traffic," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 920–939, 2011.

[17] T. D. Räty, "Survey on contemporary remote surveillance systems for public safety," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 40, no. 5, pp. 493–515, 2010.

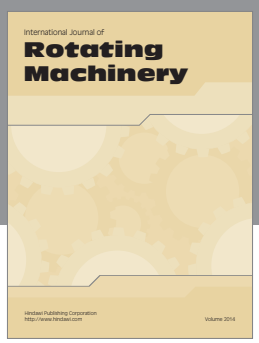
[18] KISA, *Global Information Security Industry Trend Survey Research*, Korea Internet Security Agency, 2013.

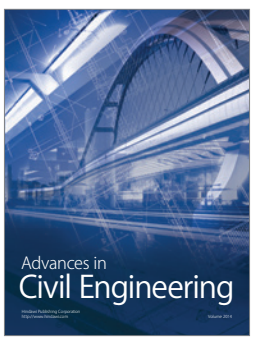
[19] KOTRA, International Business Product Information, Market Trends, 2013, http://tradedoctor.kotra.or.kr/.

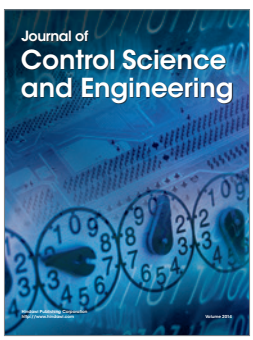
[20] T. Seo, S. Lee, B. Bae, E. Yoon, and C. Kim, "An analysis of vulnerabilities and performance on the CCTV security monitoring and control," *Journal of Korea Multimedia Society*, vol. 15, no. 1, pp. 93–100, 2012.

[21] T. Seo, "A study on vulnerabilities of monitoring and control system based on IT convergence technology," in *Proceedings of the 6th International Conference on Multimedia Information Technology and Applications*, 2010.

[22] Trend Micro, *Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond*, Trend Micro, 2013.







Hindawi
Submit your manuscripts at
http://www.hindawi.com