Secure Video Transmission on Smart Phones for Mobile Intelligent Network

Seunghwan Choi[1,4], Sungju Lee[2], Yeonwoo Lee[3], Changsun Kim[1,4]
and Taikyeong Jeong[1,4]

[1]*Korea Electric Power Research Institute*
[2]*Dept. of Computer Information Science, Korea University, Korea*
[3]*Dept. of Computer Information Science, Sungshin Women's University, Korea*
[4]*Dept. of Electronic Eng., Myongji University, Korea*

kepchoi@kepri.re.kr, peacfeel@korea.ac.kr, yeonwoo57@sugshin.ac.kr, {cskim, ttjeong}@mju.ac.kr

Abstract

Video data delivery comes up problems of the content ownership and the privacy, and thus protecting the video data becomes important in mobile network. With the standardized protocol defined by AES-CCM, the need is to implement communication infrastructure for a next-generation mobile computing and intelligent system, i.e., Smartphone, evaluating security parameters (e.g., CP (Control Parameter), UP (Unit Parameters) and standardization it's a challenging task. The details provided in this paper are used to design a CP based secure wireless video data transmission, on basis of AES-CCM for privacy issues, considering the security level with MAC overhead.

Keywords: *Information security; Privacy protection; Smart Phones; Mobile network*

1. Introduction

With privacy involved among several nodes, or single networks, there are transmitting objects and delivery method is important part that we have to consider in order to figure out security and privacy. Recent remarkable needs for multimedia application for mobile handhelds, such as Smartphone, has a manufacturer oriented service is spread out in the market so that people like to use these devices when they use finance, purchase, travel and entertainments without deeply thinking theirs personal privacy information [1-7].

Recently, since many Smartphone use the Android operating system, it is necessary to observe the performance and security issue. In this paper, we apply the AES-CCM [8, 9] to Android platform for ensuring both confidentiality and integrity of video data. Also, we confirm that the performance of multimedia and crypto applications on Android platform for advanced mobile intelligent network.

Moreover, it is challenging issue for satisfying the performance and security requirements on mobile computing and intelligent system, in this case, Smartphone. To solve this problem, we propose evaluating security parameters (e.g., *CP* (Control Parameter), *UP* (Unit Parameters) with mobile network testing. The details provided in this paper are used to design a *CP* based secure wireless video data transmission, on basis of AES-CCM standard for privacy issues, considering the security level with MAC overhead. The choice of *CP* is to attain the run-time requirement of data transmission for *UP*.

The rest of the paper is structured as follows. Section II describes security and privacy issues while transmitted. Section III explains privacy parameters of the proposed approach. Section IV explains experimental environments. Section V and VI explains the experimental results and conclusions, respectively.

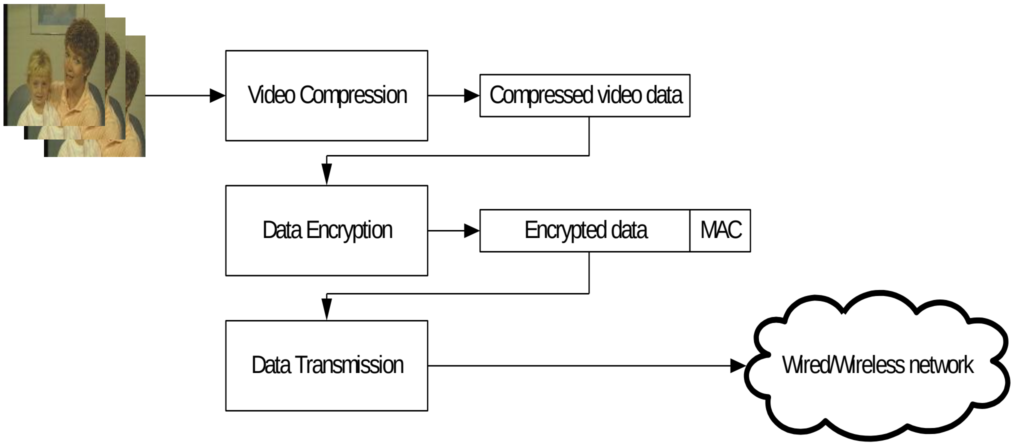

Figure 1. Privacy and Authentication Procedure for Secure Video Transmission

2. Background

2.1. Video compression and Transmission Issues

In general, digital video data can be compressed using both lossy and lossless compression technique. Lossy compression is a technique to remove spatial and temporal redundancy [7]. In video compression algorithms such as MPEG and H.264, transformation coding (*i.e.*, discrete cosine transform) and quantization techniques have been studied in order to remove the spatial redundancy. Also, motion estimation and motion compensation have been studied in order to remove temporal redundancy between frames. Lossless compression such as Huffman coding and arithmetic coding is a technique to reduce the amount of statistical entropy.

Recent development in the area of image processing, one of the best video coding standards, in terms of compression and quality is H.264 [7]. H.264/MPEG-4 Part 10 or AVC (Advanced Video Coding) is a standard for video compression, and is one of the most commonly used formats for the recording, compression, and distribution of high definition video. The coding efficiency gains of advanced video codecs such as H.264 come at the price of increased computational requirements. The demands for computing power increases also with the shift towards high definition resolutions. MPEG and H.264 are ISO (International Organization for Standardization) and ITU(International Telecommunication Union) standards for video compression. Figure 2 illustrates the H.264 video encoder.

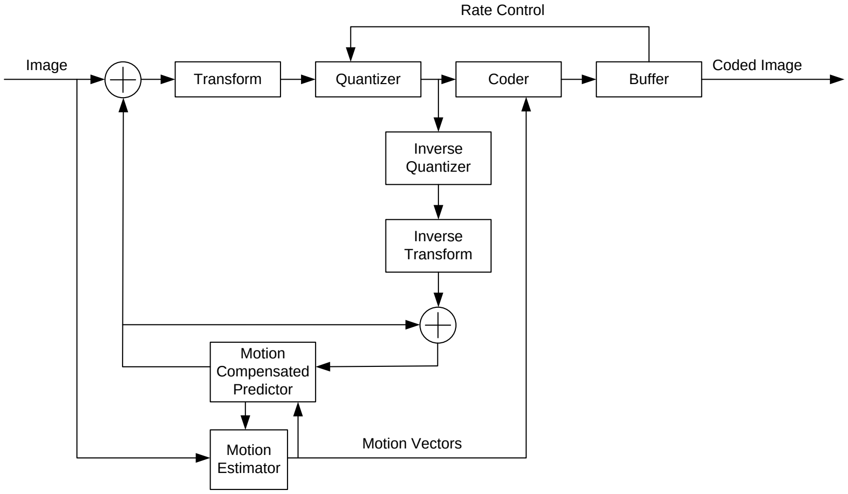

Figure 2. Encoder of H.264 [7]

2.2. Security and Privacy Issues

Although research on privacy enhancing technologies began more twenty years ago, most of the existing schemes focus on textual data and do not enough to protect multimedia. With the advance on the multimedia technology, the multimedia contents can be delivered to/from users having portable devices such as Smart phones. Multimedia data delivery raises problems of the content ownership and the privacy, and thus protecting the multimedia data becomes important in multimedia applications [1-7]. The particular challenges are not limited to the difficulties in extracting semantic information for protection, the ability to apply cryptographic primitives to high data-rate multimedia streams, basic signal processing algorithms for protecting privacy without destroying the perceptual quality of the signal, and privacy models for governing and handling privacy rights in multimedia systems [10].

In cryptography, Hash-based Message Authentication Code (HMAC) is a specific construction for calculating a Message Authentication Code (MAC) involving a cryptographic hash function in combination with a secret key. The cryptographic strength of the HMAC depends upon the size of the secret key used. The most common attack against HMACs is the brute force attack to uncover the secret key.

Block cipher modes of operation have used with block cipher such as AES [8]. For ensuring confidentiality and integrity of the data, National Institute of Standards and Technology (NIST) has proposed five modes of operations [9]. One of the five modes, Counter (CTR) mode can be used as a stream cipher, and encrypt data very fast. Another method to verify integrity is Cipher Block Chaining-Message Authentication Code (CBC-MAC), which uses the final block for verifying of the message integrity.

AES-Counter with CBC-MAC (AES-CCM) [8] is a combined encryption and authentication block cipher mode. The CCM mode specification supports either both authentication and encryption or encryption only. AES-CCM algorithm consists of two processes: (1) CCM requires two block cipher encryption operations per each block of encrypted and authenticated message; and (2) one encryption per each block of associated authenticated data (See Figure 3).

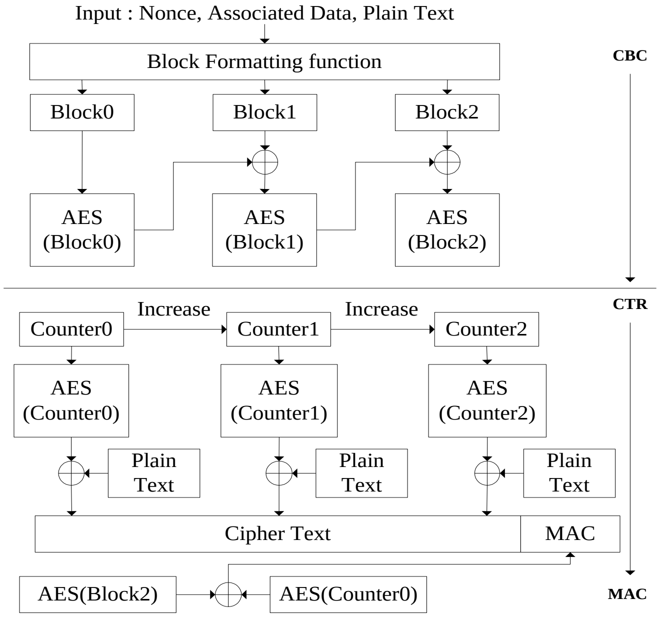

Figure 3. Block Diagram of AES-CCM [8, 9]

3. Video Authentication

3.1. Privacy Parameters

In this paper, we apply the AES-CCM in order to ensure both the confidentiality and the integrity of video data. Figure 4 shows the illustration of authentication procedures for video data. The video data is encrypted with AES, and MAC is generated by CBC mode. Also, the video data is encrypted with AES-CTR for ensuring the confidentiality of video data. To verify the MAC, the video data is decrypted with AES and the MAC' is generated by CBC mode. Finally, we confirm that the video data is not forgery, if MAC and MAC′ are completely same.

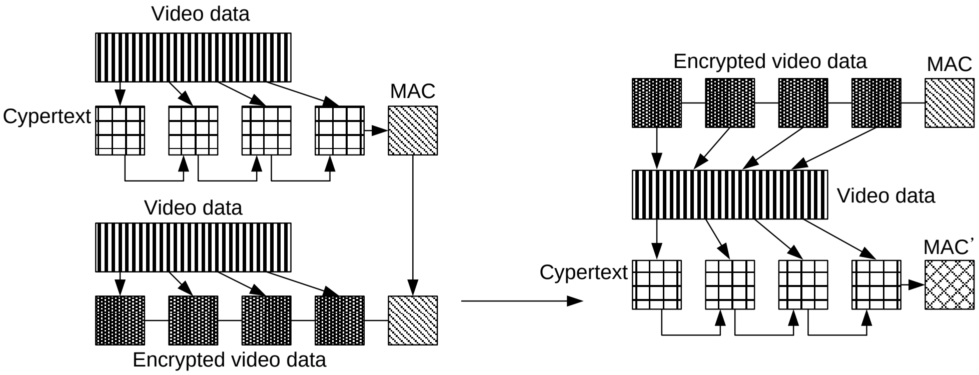

Figure 4. Illustration of Authentication Procedures for Video Data

The video data has huge amount of data, even it has been efficiently compressed. Therefore we need a way to determine the number of MAC for the while video data. For example, if video data size is 64 byte, we can divide the data 16 byte, 32 byte, 48 byte, and 64 byte. Also, the number of MAC is 4, 2, 2, and 1, respectively. It should be noted that, with increased the number of MAC, the video streaming data may enhance the error propagation. On the contrary, with decreased the number of MAC, it improve the performance due to reducing data overhead. In this paper, we define some notation as *CP* and *UP* to determine the number of MAC for the while video data. Figure 5 shows an example for behavior of *UP* (# of MAC) with *CP*.

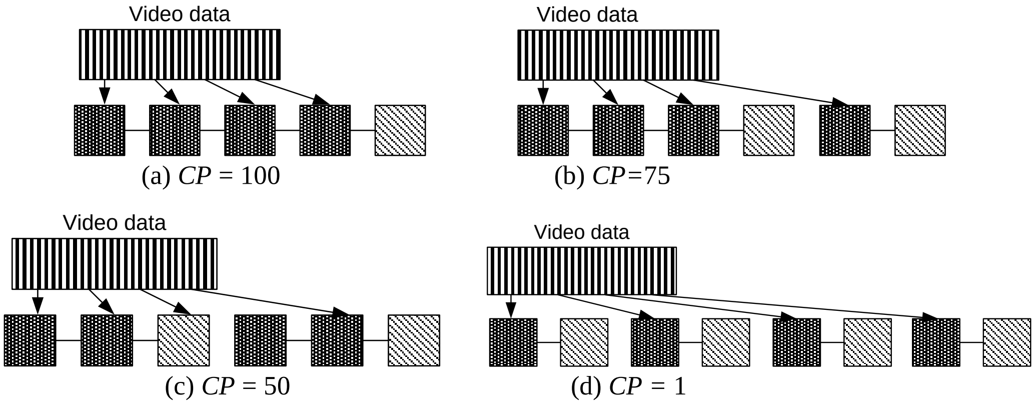

Figure 5. An Example for Behavior of *UP* (# of MAC) with *CP*

CP and *UP* is as follow Equation (1) and Equation (2). *CP* is a ratio for divide video data, where 1, 2, 3, …… ,98, 99, 100. At the same time, *UP* is defined by Equation (2) based on *CP* calculation. Note that, if *CP* is increased, *UP* is decreased and the transmission time is reduced. On the contrary, if we decrease the *CP* in order to enhance the error propagation, the *UP* is increased.

$$CP = Ratio\ for\ Divide\ vide\ data \qquad \text{Equation (1)}$$

$$UP = \left\lceil \frac{\lceil Video\ Data\ Size \rceil}{\left\lceil Video\ Data\ Size \times \frac{CP}{100} \right\rceil} \right\rceil \qquad \text{Equation (2)}$$

3.2. Analysis of Privacy Parameters

First, we analyze the relationship between the privacy parameter, transmission time and security level as shown in Figure 6. Note that, the *CP* affects not only the transmission time, but also the security level. For example, the decreased number of MAC with increased the *CP*, the security level may decrease due to not enough the number of MAC. Therefore, we define the security level as equation (3).

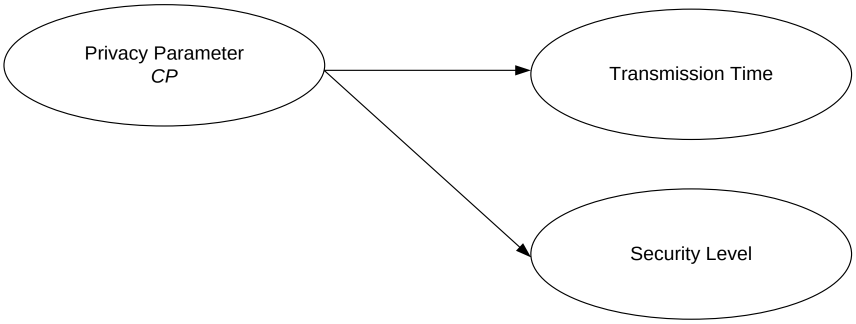

Figure 6. The Relationship between Privacy Parameter, Transmission Time and Security Level

$$Security\ Level = \frac{1}{CP} \times 100 \qquad \text{Equation (3)}$$

Also, the transmission time depends on the transmitted data size, and network bandwidth. The transmission time is increased with the decreased the *CP*(increased the UP) due to increased data overhead, and the decreased network bandwidth. Therefore, we represent the transmission time as Equation (4), where the Block Size is 256 byte.

$$Transmission\ Time = \frac{UP \times Block\ Size + Compressed\ Video\ Data}{Network\ Bandwidth} \qquad \text{Equation (4)}$$

To determine the *CP*, we use the analysis for the relation of transmission time and security level with *CP*. Figure 7 shows the proposed system for secure video transmission on smart phones. Since we consider both the transmission time and the security level, the proposed system can provide the high performance with satisfying the security level. For example, if the network environment (*i.e.*, network bandwidth) was given, we determine the optimal *CP*, and then the video data can be fast and secure transmitted via wired/wireless network.

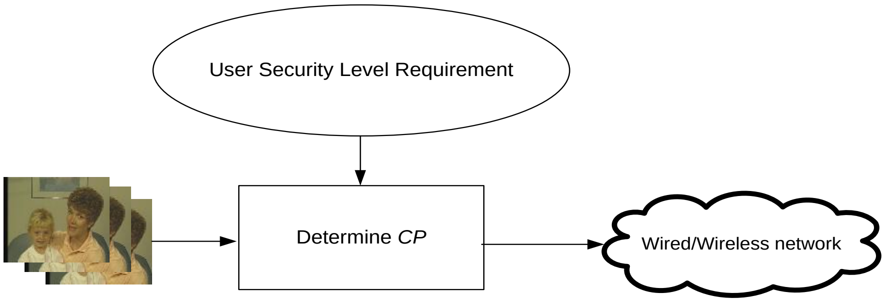

Figure 7. The Proposed System for Secure Video Transmission on Smart Phones

4. Test Environments

4.1. Testing Platform Environments

Android platform requires an environment for JAVA programming, that installation of JAVA Eclipse, JRE (JAVA Runtime Environment), and JDK is required in order to perform the applications on it [11]. In this paper, we use an Android emulator for validation of proposed approach as shown in Figure 8. To use the Android emulator, Eclipse and the Android SDK should be connected after installation of JDK, Eclipse, and ADT (Android Development Tool). Note that, Android SDK includes the development library, support documents, support tools for development. Finally, we use the Android emulator by AVD (Android Virtual Device) in the Eclipse program. Although, Android emulator is a virtual software emulator, it can provide the real environment as same as android based device.

Figure 8. Android Emulator for Validation of Proposed Approach

However, since the real device depends on the hardware specification, the application should be test on target device using emulator for high accuracy results. In our experimental environments, the host spec was as shown Table 1, and conducted on Android 2.2 (API Level 8) having ARM processor, and the resolution was HVGA (320 × 480).

Table 1. Host Spec.

OS	Windows 7
Processor	Intel(R) Core(tm) i5 CPU 750 @ 2.67GHz
RAM	4.00GB
System Type	32bit OS

4.2. Video Test Data

We used the H.264 compression algorithm, and various video data. We selected CIF-size akiyo, carphone, bridge_close, garden, mthr_dotr, and tennis from the image/video data set [12], and modified the size as 320 × 240. Figure 9 shows these input data.

(a) (b) (c)

(d) (e) (f)

Figure 9. Video Data Set [12]

5. Results and Discussion

In this paper, Android Emulator was used for experiments, and the size of experimental video image was 320✕240 and the frame rate was 30 frames/second. The total size of frames was 3.46 MB except headers [12], and the network bandwidth was 100Kb/sec.

Table 2 shows the execution time and transmission time with *CP* and *UP,* when AES-CCM standard tested on Android emulator. The AES-CCM execution time is 2.757 msec on Android emulator without considering *CP* and *UP*. However, the transmission time depends on the *CP* and *UP*. If *CP* is increased, *UP* is decreased and the transmission time is reduced. On the contrary, if we decrease the *CP* in order to enhance the error propagation, the *UP* is increased. Therefore to meet the latency of the video data transmission, we can set the optimal *CP* with enhancing the error propagation. For example, we can set the *CP* as 100 for high performance in the stable network such as wired network. On the contrary, if the network is not stable, we may set the *CP* as 1 for enhancing the error propagation.

Table 2. AES-CCM Execution Time and Transmission Time with *CP* and *UP*

CP	**Execution Time (msec)**	***UP* (# of MAC)**	**Transmission Time (msec)**
1	2.757	100	16
4	2.757	25	4
16	2.757	7	1.12
64	2.757	2	0.32
100	2.757	1	0.16

Figure 10 shows the execution and the transmission time with *CP*. Note that the ratio of the execution time was rapidly down with increased *CP*. We should carefully set the *CP* to provide better performance. Also, to satisfying the latency requirements, we may set the increased *CP* to reduce the MAC overhead. Therefore we can meet the real-time performance with satisfying the enhancing the error propagation.

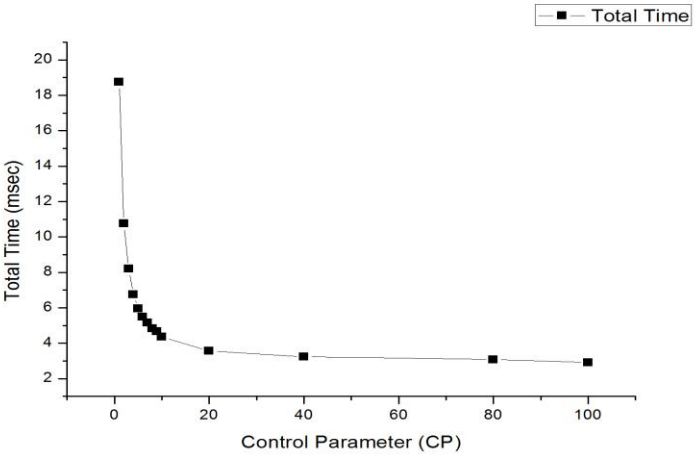

Figure 10. Test Results of the Total Execution and Transmission Time with *CP*

6. Analysis of Tradeoff the Time and Security

We analyzed system performance and the security level with *CP* regarding the execution time. To analyze the each performance, we defined the performance which projected by time-domain as Equation (5). Figure 11 shows the trade-off between this time performance and the security level. It should be noted that we normalized the time performance and the security level based on *CP* 100(*i.e.*, the number of MAC was one). In the increased *CP*, we observed that it sensitively affected the time performance and the security level. Also, the cross point was founded at *CP* 4~6 in Figure 11. Therefore, we should carefully determine the *CP* in order to improve the both the time and the security level.

$$Time\ Performance = \frac{Time\ at\ CP\ 100}{Total\ time} \qquad \text{Equation (5)}$$

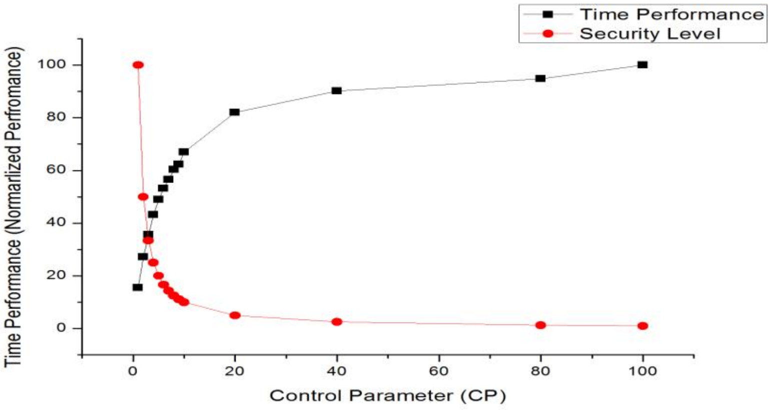

Figure 11. Tradeoff between Time and Security

Finally, we carefully configured the *CP* to improve the time performance and the security level. To analyze the trade-off the time performance and the security level collectively, we used the Equation (6). Figure 12 shows the collective performance of time and security. In these environments, we can maximize the performance with lowest *CP*, and the system has the largest number of MAC. Therefore, with optimal *CP*, we can implement that the AES-CCM is applied to Mobile Android platform for ensuring both confidentiality and integrity of video data under the real-time performance.

$$\text{Total System Performance} = \frac{\text{Time Performance} + \text{Security Level}}{2} \qquad \text{Equation (6)}$$

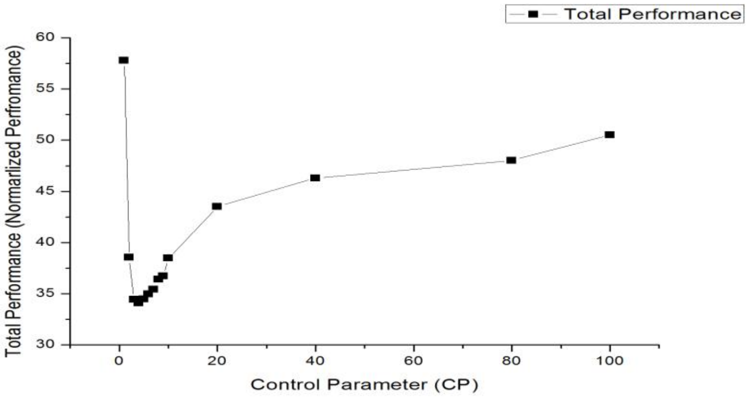

Figure 12. Analysis of Collective Performance of Time and Security

7. Conclusions

We have chosen security parameters (*CP* and *UP*) based on the AES-CCM standard, which is a developed privacy standard. With the standardized protocol defined by AES-CCM, the need is to implement communication infrastructure for a next generation mobile computing and intelligent system, i.e., Smartphone, evaluating security parameters and standardization it's a challenging task. We have confirmed that the AES-CCM is applied to Mobile Android platform for ensuring both confidentiality and integrity of video data.

Acknowledgement

This work was supported by the IT R&D program of The MKE/KEIT. 10040191, the development of Automotive Synchronous Ethernet combined IVN/OVN and safety control system for 1Gbps class. The circuit was designed at IC Design Center.

References

[1] J. Son, H. Lee and H. Oh, "PVR: a novel PVR scheme for content protection", IEEE Tr. Consumer Electronics, vol. 57, no. 1, **(2011)**, pp. 173-177.
[2] H. Sohn, Y. Ro and K. Plataniotis, "Content sharing between home networks by using personal information and associated fuzzy vault scheme", IEEE Tr. Consumer Electronics, vol. 55, no. 2, **(2009)**, pp. 431-437.
[3] S. Lian and Z. Liu, "Secure media content distribution based on the improved set-top box in IPTV", IEEE Tr. Consumer Electronics, vol. 54, no. 2, **(2008)**, pp. 560-566.
[4] Y. Zou and T. Huang, "H.264 video encryption scheme adaptive to DRM", IEEE Tr. Consumer Electronics, vol. 52, no. 4, **(2006)**, pp. 1289-1297.
[5] S. Lian, Z. Liu, Z. Ren and H. Wang, "Secure advanced video coding based on selective encryption algorithms", IEEE Tr. Consumer Electronics, vol. 52, no. 2, **(2006)**, pp. 621-629.
[6] G. Kim, D. Shin and D. Shin, "Intellectual property management on MPEG-4 video for hand-held device and

mobile video streaming service", IEEE Tr. Consumer Electronics, vol. 51, no. 1, **(2005)**, pp. 139-143.
[7] B. Furth and D. Kirovshi, "Multimedia Security Handbook", CRC Press, **(2005)**.
[8] W. Stallings, "Cryptography and network security", Pearson, **(2006)**.
[9] N. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", NIST Special Publication 800-38C, **(2002)**.
[10] S. Senching, D. Cheung, K. Deepa and S. Andrew, "Enhancing Privacy Protection in Multimedia Systems", Hindawi Publishing Corporation EURASIP Journal on Information Security, **(2009)**.
[11] http://developer.android.com.
[12] http://media.xiph.org/video/derf/.

Authors

Seunghwan Choi

Seunghwan Choi received the M.S. degree from the Dept. of computer Eng., Chungbuk University. He is a Ph.D. candidate at the Dept. of Electronic Eng., the Myongji University. He performed research in the area of a log analysis model for the inference of intrusion detection. He is a Principal Researcher at Software Center (KEPRI), working on integrated operating system for Smart Grid and development of portal for demand based on demand forecasting.

Sungju Lee

Sungju Lee received his B.S. and M.S. degrees from Korea University, Korea in 2006 and 2008, respectively. He is currently in Ph.D. program in the Department of Computer and Information Science at the Korea University. His research interests include Biometrics, Information Security, and Energy-efficiency of Image Compression.

Yeonwoo Lee

Yeonwoo Lee received her B.S. degree in Computer Science from Sungshin Women's University, Korea in 2011. Currently she is studying for her M.S degree in Information Security at the same university. Her research interests include Security Architecture and Privacy Protection

Changsun Kim

Changsun Kim received his B.S. degrees from Andong National University and M.S. degrees from SungKyunKwan University, Korea in 1997 and 2009, respectively. He is currently in Ph.D. student in the Department of Electronic Engineering at Myongji University. His research interests include Software Process, Embedded Software, Information Security, Quantum Information Science and System Semiconductor (SoC).

Taikyeong Jeong

Taikyeong Jeong received the Ph.D. degrees in the Department of Electrical and Computer Engineering from the University of Texas at Austin, in 2004. He also worked for IBM Austin Research Laboratory where he joined the high performance communication chip design and systems. Prof. Jeong is currently an Associate Professor with the Department of Electronic Engineering at Myongji University. His research interests include low power design, computer architecture. He is a member of IEEE, IEICE, and IEE