An Experimental Study of Performance, Energy Consumption, and Video Quality for Secure Mobile Video Communications

A Master's Thesis

Submitted to the Department of Computer Science and Engineering and the Graduate School of Yonsei University in partial fulfillment of the requirements for the degree of Master of Science

Joosung Lee

June 2013

An Experimental Study of Performance, Energy Consumption, and Video Quality for Secure Mobile Video Communications

Joosung Lee

The Graduate School

Yonsei University

Department of Computer Science and Engineering

This certifies that the master's thesis

of Joosung Lee is approved.

Thesis Supervisor: Kyoungwoo Lee

_____

Thesis Committee Member : Seon Joo Kim

_____

Thesis Committee Member : Bernd Burgstaller

_____

The Graduate School

Yonsei University

June 2013

Contents

List of Figures and Tables

Abstract

An Experimental Analysis of Performance, Energy Consumption, and Video Quality for Secure Mobile Video Communications

Joosung Lee

Dept. of Computing Science and Engineering

The Graduate School

Yonsei University

Thanks to technology advances, lots of mobile applications have been developed and introduced. In particular, multimedia applications are receiving lots of attentions since advanced technologies can allow expensive and complex computations to be executed in mobile embedded systems. The mobile video communication occasionally deals with personal information and even classified information. Thus, the encryption of video data becomes indispensable. Aspect of security level, the higher security requires more overheads in terms of performance and energy consumption. Lower security level could be too weak to

protect the video information. So it is necessary to define the proper security levels. However, they demand high-energy consumption since video coding and cryptography tasks are significantly complex and expensive. Energy efficiency is the utmost key factor to be considered in mobile platforms due to the limited battery. In this thesis, we conduct various experiments by configuring parameters of H.263 video codec and those of AES(Advanced Encryption Standard) cryptographic algorithms in Android-running smartphones. Through the experiments, we investigate trade-offs and implications among video quality, performance, and energy consumption. Based on experimental results, we discuss the potential methods of minimizing the energy consumption while maximizing the video quality and the security level for secure mobile video communications.

Key words: secure video communication, android, smartphone, H.263+, encoding, decoding, encryption, decryption, QoS, performance, mobile embedded system

Chapter 1

Introduction

As spreading of mobile embedded systems, various mobile applications are being developed and introduced. Among them, the applications deploying video information are being used broadly. Video communication applications and video conferencing applications the video information using applications have been already commercialized in the market. Further, mobile video communications are available and keep changing humans' lifestyle: they work through video conferencing and appreciate the video entertainment anytime anywhere. Those easily available video applications are becoming more popular thanks to embedded devices such as smartphones.

The mobile video applications contain entertainment delivering pleasure and convenience, and also contain severe contents such as military-classified video information in the battlefield applications, and private and critical video information of patients in medical applications. Furthermore, video streaming and video conferencing applications also handle private information or confidential video data of companies. So it is a necessity addressing the secure mobile video applications.

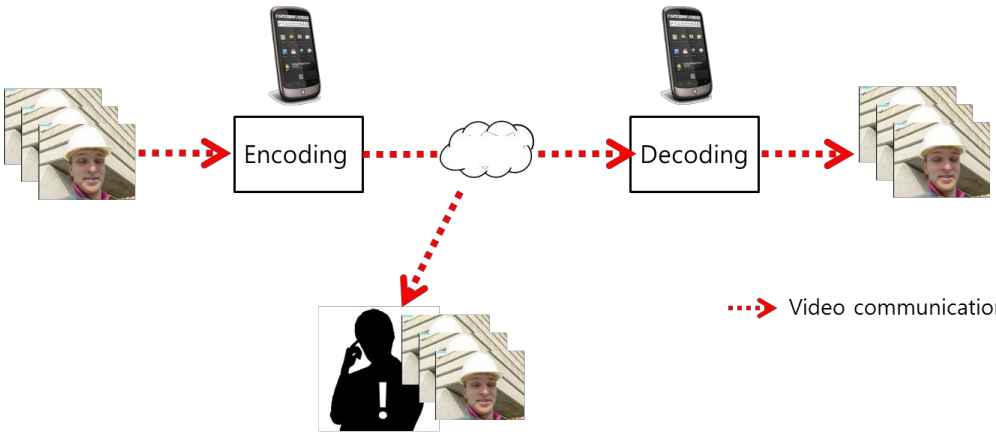
[Figure 1] Leaked video from US military [1]

For instance, [Figure1] shows the leaked video from the US military at 2007. Two Reuter journalists were killed by Apache helicopter and dozens of Iraqis were killed also. US military received severe criticism for the case. Those videos should not be leaked because it is military-classified information. And this is one of good reason why we have to protect the video information.

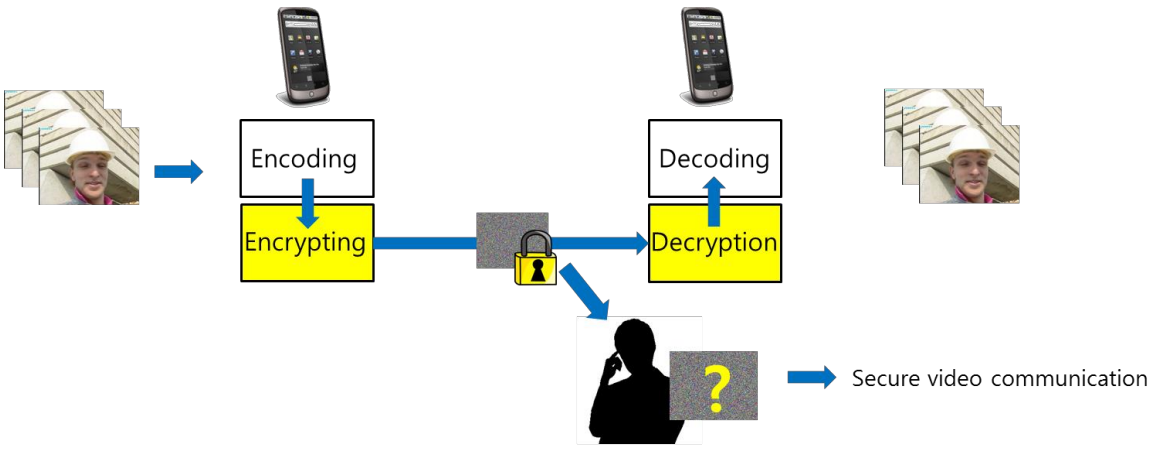
However, in these video applications, the security is not treated as important. On account of mobile embedded devices' poor bandwidth, most of video application researches are being carried out to deal with compression performance

under the QoS[2][3][4].

We pay attention to that in video applications security does not care as much as performance of compression or QoS. We searched former researches about video communications and video conferencing and analyzed the process of secure mobile video communication through the experiment. Moreover, we contributed that we made the testing environment of measuring energy consumption, execution time, QoS, and secure degree for each encoding, decoding, encryption, and decryption. It's expected that the result from previous tests can be used for further work.



(a) Common video communication



(b) Secure video communication

[Figure 2] Secure video communication

[Figure2] shows the draft of secure mobile video communication process. In the (a), the dot-line shows the process of common video communication that does not care about security. In common video communication, if the malicious attacker

tries to intercept the encoded video information, he or she could easily extract what the contents is from the data by simple decoding. In the (b), the full-line shows the secure video communication process which added encryption/decryption module. In this case, the malicious attacker could not easily get the information from the encoded data, even if he or she tries decoding. So that secure mobile video communication could protect the private or important information.

Nevertheless, adding security module on video communication application could cause mass overhead on execution time and energy consumption. To solve this problem, the quality degradation or security degree degradation are unavoidable. Thus, we experiment by adjusting several parameters to reduce the overhead during maximize the QoS and security degree. Our first purpose is measuring and finding the connection among the execution time, energy consumption, QoS, and compression ratio of the secure mobile video communication application. Further by researching those connections, searching for the conditions or method to minimizing the overhead while maximizing QoS and security degree is our final purpose.

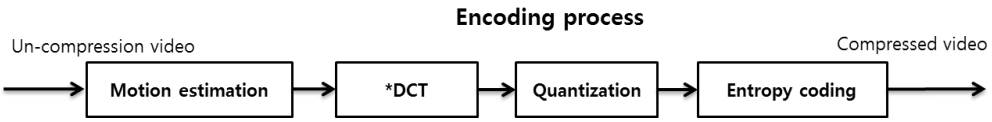
Chapter2

Related work

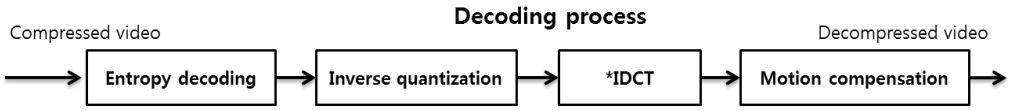
Our research and experiments are using several modules that perform specific function such as compression, decompression, encryption, and decryption of video information. At the beginning of the experiments, the video is encoded using TMN3.2(H.263+)[5] codec. And then we used AES cipher module[6] for encrypting and decrypting the video information data.

2.1 H.263+ video codec

TMN3.2 codec is widely using H.263+ codec module. The figure shows draft process of encoding and decoding of H.263+. H.263+ basically can control the quantization scale, IP ratio, and motion estimation method. Therefore, it is necessary to look into these factors.



(a) Encoding process



(b) Decoding process

* DCT : Discrete Cosine Transform
*IDCT : Inverse DCT

[Figure 3] Process of encoding and decoding process using H.263+

● Quantization scale

Quantization scale is most influential parameter in video quality. If the quantization scale gets bigger, the loss rate of video information increases together. It is expected that compression ratio could be higher during video information loss[7]. So degrading quantization scale is excelsior aspect of compression ratio than other factors. As compression ratio gets higher by adjusting quantization scale, it can be instructive for the execution time and energy consumption. But overloaded quantization scale could make worse for the QoS because of loss of video information. In the worst case, the video could not be discerned by human visual

system. So that, quantization scale modification should be carefully controlled by considering correlation between compression ratio and quality of video.

- **IP ratio**

IP ratio means the ratio between Intra frame(I-frame) and Predictive frame(P-frame). In H.263+, user can define the GOP (Group of pictures) to control the number of I-frames. That is if GOP set to be the 10, it means only one I-frames would be in each 10 frames. The other 9 frames would be P-frames. Due to I-frames' data size being bigger than P-frames, ascending IP ratio can make compression ratio higher. Getting higher compression ratio through the IP ratio adjusting have less affection to the QoS than quantization scale adjusting, but computing P-frames bring higher computational overhead than I-frame does as P-frame making process needs extract motion estimation information from the precedential I-frames. Adjusting IP ratio cause less degradation of QoS but computational burden could be arising. So should be carefully controlled by consideration of computational overhead.

- **Motion estimation method**

TMN3.2 codec provide two kinds of motion estimation algorithm, full

search and fast search. Full search method searches whole frames thoroughly, so compression ratio could be better but computational burden could be bigger than other motion estimation algorithms. Fast search method searches important image data selectively, so computational burden could be reduced compare to full search, but compression ratio could be worsened. When choosing motion estimation method, we have to consider about increasing compression ratio by using full search or reducing compression ratio by using fast search.

2.2 Encryption and decryption method

Encrypting and decrypting method can be classified as symmetric and asymmetric.

Asymmetric encryption and decryption scheme use different keys between encryption and decryption process. RSA(Rivest Shamir Adleman)[8], DSA(Digital Signature Algorithm)[9], ECDSA(Elliptic Curve Digital Signature Algorithm)[9] schemes are one of the widely using asymmetric algorithm. The energy consumption and execution time of asymmetric cipher algorithm is also different between encryption and decryption. Commonly, asymmetric cipher algorithms work better than symmetric cipher algorithms in terms of security

degree, but in terms of performance overhead, asymmetric cipher algorithms takes more overhead than symmetric cipher algorithms especially on the encrypting side[10].

Symmetric cipher methods use same key between encryption and decryption side. Symmetric algorithms can be classified as block-based and stream-based. Block-based cipher scheme divides plain-text as same size block and then encrypting. And stream cipher scheme is usually used to make streaming data to cipher-text like video data bit by bit. DES, 3DES, AES, and BLOWFISH algorithms are belong to symmetric cipher scheme, and we used AES scheme in our experiments. AES(Advanced Encryption Standard)[6] is known for energy efficient scheme compared to other symmetric cipher schemes. [11] Basically, AES provides 128, 192, and 256 bits of keys, and ECB (Electronic codebook), CBC (Cipher-block chaining), CFB (Cipher feedback), and OFB (Output feedback) modes. Originally, these modes are block-based algorithms. However, CFB mode could be used stream-based-likely. We used 128 and 256 key size, and ECB, CFB modes to encrypt and decrypt the information.

[Table 1] References of video encryption

Paper	Experiment	Merit	Weakness
K Lee et al. 2005 [13] Encryption energy consumption. QnS (Quality and Sequrity) concept	Monitoring energy consumption	Experimental analysis Suggest new metric (QnS)	Experimental analysis Suggest new metric (QnS)
A Massoundi et al. 2008 [19] Compare and classify Selective encryption schemes. Specific classification method.			
F Liu et al. 2010 [2] Suggest the division of Joint-Compression and encryption Algorithm and Compression independent encryption Algorithm.			
Z Liu et al. 2004 [15] Concealing(XOR) motion vector of video. Weaken the spatial domain (scrambling).	Reasonable level of visual degradation and 32-16 times performance increase.	Intend to overcome the limitation of MV (spatial domain).	Entropy part is weak. Compression ratio increases about 100 times.
Y LI et al. 2005 [17] In H.264, encrypting over Intra prediction mode, Inter prediction mode, Transform coefficient and motion vector and get the security complexity and compression ratio.		Addressing multiple side of video information.	Conclusion is weak. Not including experiment.
Y Zou et al. 2006 [14] In H.264, partially encrypt VCL unit to reduce the overhead.		H.264 specification NAL unit and VCL.	Codec specific. Too simple idea.
S Li et al. 2007 [16] Suggest concept of Perceptual video encryption. Encrypt DC part of Intra DCT coefficient, rest of DCT coefficient, sign bits of ESCAPE DCT coefficient, and MV.	Encrypting in Motion vector is weak and visible so need the other factor simultaneously.	Apply new idea. Can cnotrol visual degradation.	Weak explanation of implementation. Only work in FLC.
D Wang et al. 2009 [18] In H.264, using RC4, prediction mode encryption. And summary about energy consumption, security, complexity and compression ratio.	Baseline profile of JM86 encoder, OpenSSL RC4 library	H.264 specification inter prediction of intra frame.	Codec specific

2.3 Full Encryption and selective encryption

Some of the research of video encryption is about the necessity of encrypting whole video data. Called VEA(Video Encryption Algorithm)[12] is one of them. In the video data, there are stand-alone data like I-frames. The I-frames contains each frame's own data which is recognizable. And there are P-frames that could not be recognized alone because P-frame contains the information about the difference between current frame and precedence I-frame. That is to say that the selective encryption scheme means only encrypting I-frames and intra coded blocks in the P-frames, where that information is recognizable by itself. By the selective encryption, it is expected to be beneficial on the aspects of execution time and energy consumption. But actually, it is not that much beneficial than expected[10]. For example, the research comparing the energy consumption between full encryption scheme and selective encryption scheme only shows 2.4% profits. This value is too small so we have to consider that getting 2.4% benefit of energy consumption by taking degrade of security degree[13]. Therefore, we use full encryption scheme because of those reasons.

By the way there are other selective encryption schemes. Y Zou et al,[14]. suggested VEA alike video encryption scheme. The output of H.264 is NAL(Network Abstraction Layer). In the NAL unit, there are VCL(Video Coding Layer) and non-VCL. This scheme proposes that only encrypting VCL unit, because important video data are in the VCL, and non-VCL only contains

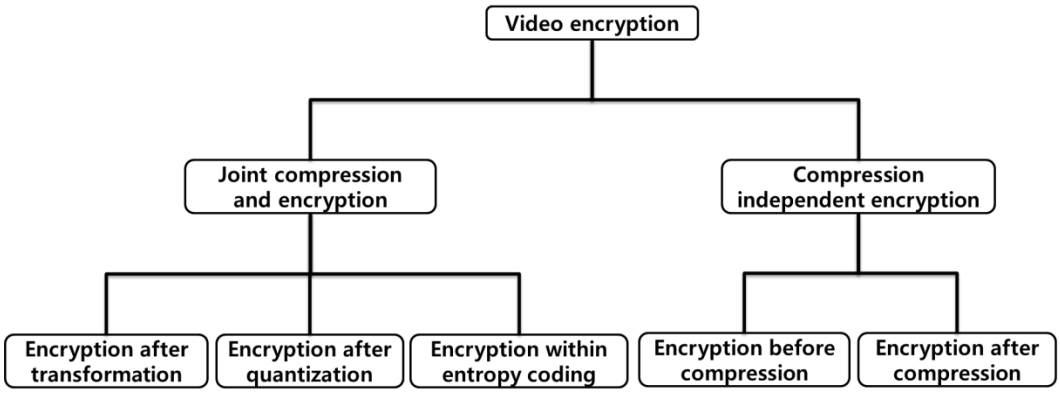
enhancing supplements. Also There are encryption schemes only encrypting motion vectors. Z Liu et al.[15] suggested encryption scheme that concealing motion vectors and scrambling to reduce the spatial information of video. This could increase visual clearness highly, but it could cause compression ratio degradation about 32~16 times. Similarly, S Li et al.[16] suggested the concept of perceptual encryption which encrypt not only motion vectors but also DC part of Intra DCT coefficient, rest of DCT coefficient, and sign bits of ESCAPE DCT coefficient. Encrypting in motion vector is weak and visible so need the other factor simultaneously. Thus, it could be the good way to reducing visual visibility. There are other kinds of encryption schemes using codec specification. Y Li et al.[17] suggested intra prediction mode encryption likely to D Wang et al.[18] It is efficient and easy to implement but the weakness is codec dependency is exist.

As mentioned previously encryption schemes are compression dependent encryption schemes.

Through entropy coding process, there are MHT encryption scheme. For the encryption, it makes multiple Huffman table to encrypt video information at the entropy coding stage. Encryption done with entropy coding could be classified as joint compression and encryption scheme.

Video encryption schemes could be classified by when encryption takes in. There are Joint compression which encrypt at the compression time, and compression independent encryption scheme which encrypt at the pre or post of

the compression[2][19]. [Figure4] shows the taxonomy diagram of video encryption scheme.



[Figure4] Taxonomy of video encryption schemes

There are encryption before compression schemes and encryption after compression schemes in the compression independent encryption. And in the Joint compression and encryption, there is encryption after transformation schemes, encryption after quantization schemes, and encryption within entropy coding schemes. Previously mentioned MHT scheme could be classified as encryption within entropy coding scheme also.

Chapter3

Problems and issues

There are several problems in secure mobile communication that does not occur in the common video communication due to intensify the security. Those problems make many commercial applications to abandon the security protection. Moreover, we have to take a look at the reducing energy consumption and performance overhead in the secure mobile video communication.

3.1 Problems of secure video communications

As mentioned from the introduction, adding secure module could cause additional overhead for the energy consumption and execution time. Unlike common video communication, secure video communication needs to consider about not only encoding and decoding but also encryption and decryption.

In secure mobile video communication, commonly, the execution time using for encryption and decryption are linearly proportional to encoded video information's size. For these reasons, to maximize efficiency of execution time, the compression ratio has to be maximized.

Energy consumption also shows linear proportion relationship to the execution time. That is, if the execution time takes longer and longer, the more energy would be consumed. Same as execution time, to maximize energy consumption, the compression ratio should be maximized.

However, if the compression ratio gets too large, the video quality could be lost. In that case, Human visual system could not recognize the video contents. Or the computational burden of compression could be raised.

3.2 The necessity of reducing energy consumption

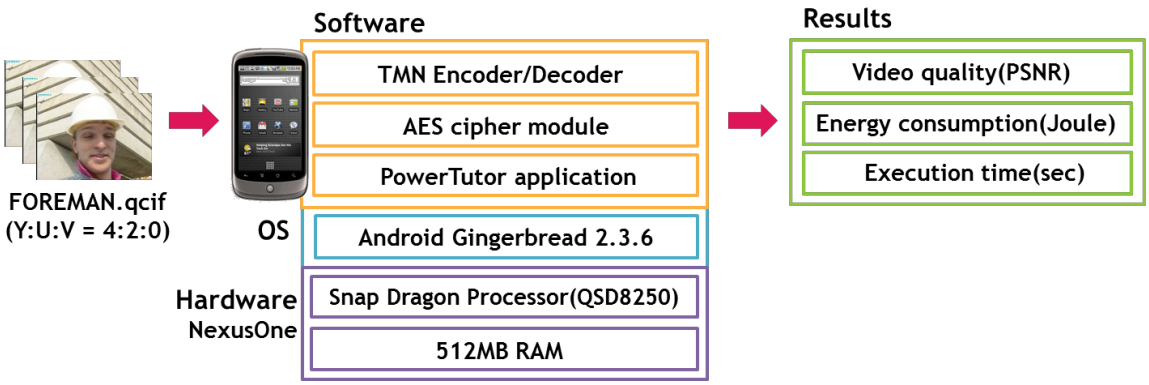
The mobile embedded systems or smartphones are using battery, so its power supply is very weak and restricted[20]. Consideration of this limited capacity of battery, we need to reduce the energy consumption of mobile applications. Generally, mobile video application uses much energy, because the process of video encoding and decoding takes much of energy. If the security module were added to this process the energy consumption would be increased because of computational burdens of encryption and decryption mentioned. Therefore, in the secure mobile video communication, the research of reducing energy consumption should be fulfilled. Especially, maximizing the security during minimizing the increase of energy consumption is the best.

Chapter4

Experiments

We fulfilled experiments on the actual devices to get the data from secure mobile video communication, by adjusting several parameters mentioned in the introduction. And looked into the effect of adjustment of those parameters.

4.1 Experimental environment



[Figure 5] Experimental environment of secure video communication

The Google reference phone and HTC Nexus One were used for the experiments. Nexus One uses Snap Dragon CPU (QSD8250) and 512MB memory, and the OS is Android Gingerbread 2.3.6 version. The FOREMAN.QCIF (300 frames, 11MB) the QCIF(Quarter Common Intermediate Frame, 176x144 pixels) sized video is used for experiments. And TMN3.2 encoder, decoder codec is used as video codec. We did to the similar experiments on the several video sequences like AKIYO.QCIF and NEWS.QCIF. Therefore, the experimental results were almost resembles each other and the movement amount of other video sequence were too small so the motion estimation and motion compensation process were not that much than FOREMAN.QCIF. FOREMAN.QCIF video sequence contains moderate movement so the experimental result could be more meaningful.

In the four stage of secure video communication, we controlled several parameters, and in same parameters, we experimented 100 times and calculated the average to reduce the errors. PSNR(Peak Signal to Noise Ratio) was obtained from the TMN codec, and get the energy consumption data from the PowerTutor[21].

The experiment is about the encoder and decoder being controlled by quantization scale, IP ratio, and motion estimation. And the experiments about the encryption and decryption are done by same codec parameters and four security parameters as ECB/128bit, ECB/256bit, CFB/128bit, and CFB/256bit.

4.2 Encoding, decoding, encryption, and decryption

Video communication, encoding and encryption stage are done in sending side, and decoding and decryption is done in the receiving side. Therefore, we divided the sending and receiving to observe the performance, energy consumption relationship between encoding and encryption for the sending side and decoding and decryption for the receiving side.

First of all, look into the stage of encoding and encryption is like as shown in the [Table 2]. The experiment are done by restricting IP ratio to 10, motion estimation is set to be the fast search, and quantization scale is controlled as 1, 4, 8, 12, 20, 31. The encryption mode is CFB and the key is 256bit.

[Table 2] Execution time and energy consumption of encoding and encrypting

Quantization scale	1	4	8	12	20	31
Encoder execution time (sec)	42.2	34.7	31.8	29.7	26.1	22.7
Encryption execution time (sec)	4.20	1.10	0.54	0.37	0.22	0.16
Execution time ratio (%)	9.95	3.17	1.70	1.25	0.84	0.70
Encoder energy consumption (J)	21	17	16	15	13	11
Encryption energy consumption (J)	1.67	0.45	0.23	0.15	0.1	0.07
Energy consumption ratio (%)	7.95	2.65	1.44	1.00	0.77	0.64

The encryption result shows that 2.95% of the execution time and 2.41% of energy consumption over encoding. Therefore, encrypting the video takes very small amount of the execution time and energy consumption over the encoding as experimental results. However, if the quantization scale is 1, the biggest data-the maximum data, the execution time and energy consumption overhead goes up to 9.95% and 7.95% and the results are being non-negligible. This result seems derived from the video size after encoding stage. If the video size gets too large, it may not fit for the encrypting energy consumption and execution time.

Secondly, the [Table 3] shows the execution time and energy consumption data of decryption and decoding stage. As same as encoding and encrypting experiments, the IP ratio fixed as 10, motion estimation method is used as fast search, and adjusting quantization scale. The decrypting mode is used CFB mode, and key is used 256bit.

[Table 3] Execution time and energy consumption of decoding and decrypting

Quantization scale	1	4	8	12	20	31
Decoder execution time (sec)	3.92	2.59	2.35	2.26	2.18	2.15
Decryption execution time (sec)	4.09	1.10	0.55	0.37	0.23	0.16
Execution time ratio (%)	104.34	42.47	23.40	16.37	10.55	7.44
Decoder energy consumption (J)	1.72	0.82	0.57	0.48	0.43	0.39
Decryption energy consumption (J)	1.63	0.44	0.23	0.15	0.09	0.06
Energy consumption ratio (%)	94.77	53.66	40.35	31.25	20.93	15.38

The maximum execution time and energy consumption of the decryption state is 104.34% and 94.77% over the decoding state, and the average is 34.10% and 42.72%, it is large portion compare to encoding and encrypting case. The AES we used in our experiment is the symmetric cipher scheme, accordingly, the execution time and energy consumption of encryption side and decryption side have to be the same. But aspect of the portion, decryption causes severe overhead to the receiving side compare to decoding side. Comparing the results of [Table 2] to [Table 3], the encoding has more computational burden than decoding.

It has to be confirmed that performance overhead, execution time, and the energy consumption has linear relationship. That is if the performance overhead is reduced, then energy consumption could be reduced too. [Table 4] shows the ratio between execution time and energy consumption. Encoding and decoding is being set to be the same as former experiments, IP ratio is 10, fast search mode, and using CFB 256 mode.

[Table 4] Relationship between energy consumption and execution time

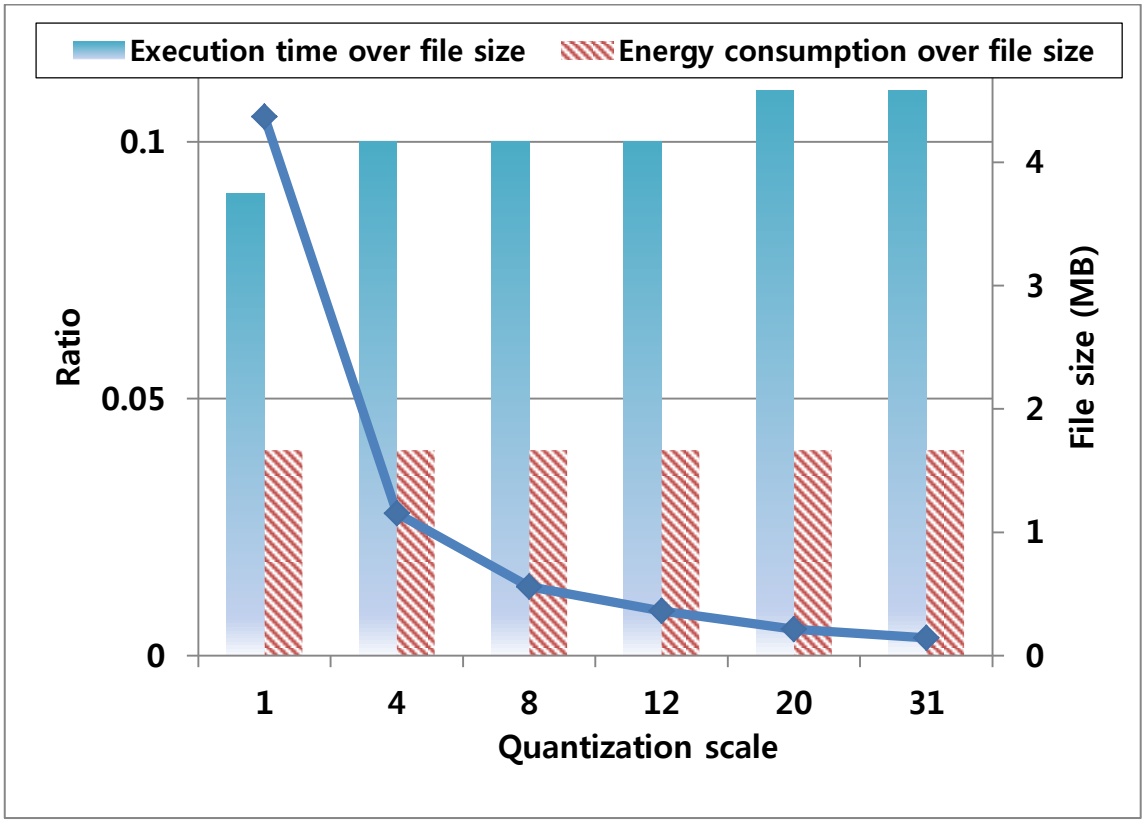
Quantization scale	1	4	8	12	20	31
Ratio of execution time over energy consumption in encoder (%)	50	49	50	51	50	48
Ratio of execution time over energy consumption in decoder (%)	44	32	24	21	20	18
Ratio of execution time over energy consumption in encryption (%)	40	41	43	41	45	44
Ratio of execution time over energy consumption in decryption (%)	40	40	42	41	39	38

As shown in [Table 4], the growth of energy consumption is tightly related with the growth of execution time. This result explains that the longer execution time means the computational burden is been increased, and increasing computing leads to the increase of energy consumption. Thus, reducing the computational burden, reducing execution time, could reduce the energy consumption.

4.3 Compression ratio and overheads

In the process of video communication, encoding is critical stage for determining overhead concerning energy consumption and performance in every following process, encryption, and decryption and decoding. The compression ratio of video information decided in the stage of encoding is directly connected to video quality. [Figure 6] is the result from the experiment with fixed IP ratio to 10 and fast search method, and it shows the execution time for decryption, energy

consumption and the ratio of that to file size. As we can see from [Figure 6] and [Table 5], execution time compared with file size and energy consumption maintain a steady rate. Moreover, we can see that steady state amount increased as the file size became larger when execution time compared with file size is same. We supposed that this result should come from the subsidiary stages such as preprocessing or post processing of the process of decryption. Thus, this results reflect the proportion of subsidiary stages such as preprocessing or post processing of the process of decryption takes a high rate as the pile capacity declines, and overhead of other stages increase when the file size become bigger. Through these results, diminishing of the file size after encoding is increasing the compression ratio of encoding as a role to reduce overhead in the process of decryption and encryption.



[Figure 6] Execution time and energy consumption over file size in decryption

[Table 5] File size, execution time and energy consumption of decryption

Quantization scale	1	4	8	12	20	31
File size after encoding (KB)	4370	1154	559	362	213	144
Decrypting execution time (sec)	4.09	1.10	0.55	0.37	0.23	0.16
Decrypting energy consumption (J)	1.63	0.44	0.23	0.15	0.09	0.06
Execution time over file size ratio (%)	0.09	0.10	0.10	0.10	0.11	0.11
Energy consumption over file size ratio(%)	0.04	0.04	0.04	0.04	0.04	0.04

There are three kinds of parameters that can control the compressibility of video in encoding. Among them, we had a research concerning the file size when the quantization scale and the IP ratio are changed. [Table 6] shows experimental result changing the quantization scale and the IP ratio using fast search. In the case of quantization scale experiment, we used the IP ratio as 10 and in the experiment of IP ratio. And we fixed the quantization scale as 5.

[Table 6] File size according to quantization scale and IP ratio

Quantization scale	1	4	8	12	20	31
File size (KB)	4370	1154	559	362	213	144
IP ratio	4	8	16	64	128	300
File size (KB)	1059	960	914	880	876	871

We should pay close attention since the improvement of IP ratio through IP ratio and the motion estimation method change do increase the computational burden of encoding. As we can assure in [Table 6], transmuting the quantization scale lessen the file size with wider variation than the IP ratio do. Therefore, to cut down the execution time and energy consumption for decryption, extending the quantization scale is more efficient way.

(a) Quantization scale 1 (b) Quantization scale 31

[Figure 7] Video quality of quantization scale 1 and 31

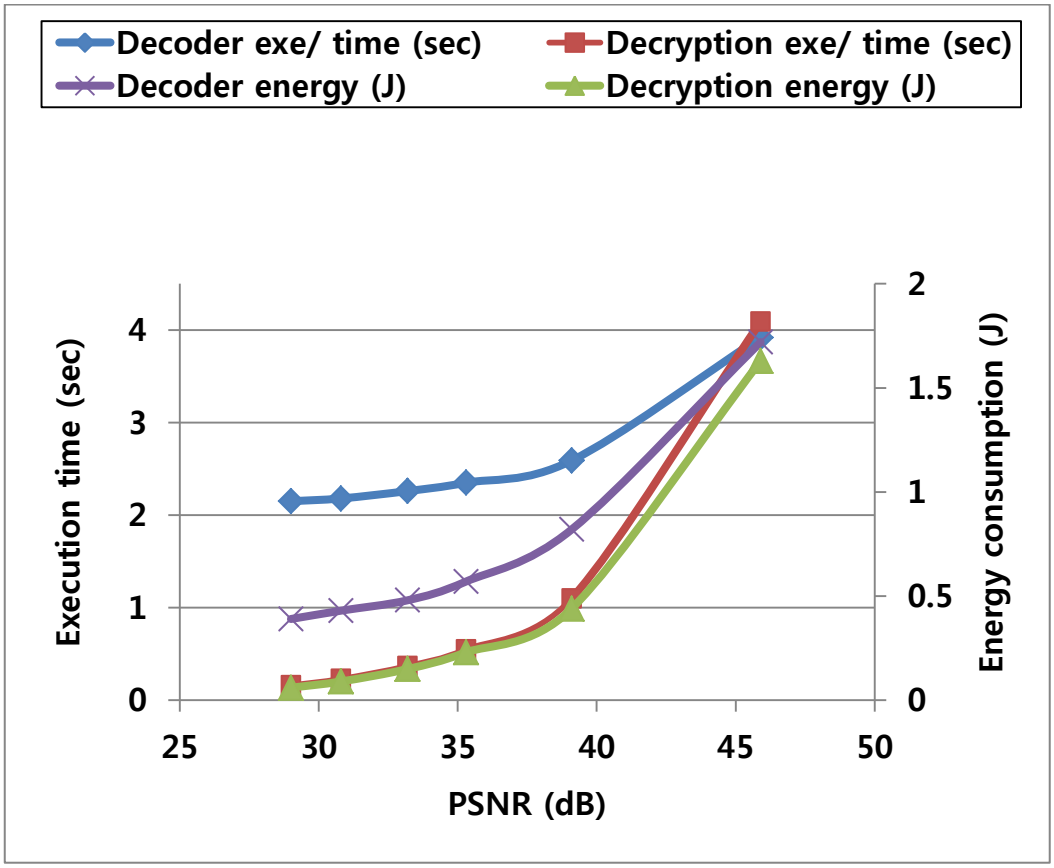
However, we should be careful, since excessive transmuting of quantization scale can change the video quality considerably. [Figure 7] shows the particular frame of encoded video experimented in [Table 6]. First picture is the result when the quantization scale is 1, and the second one is when the quantization scale is 31. This directly shows the degraded video quality caused from the excessive adjusting of quantization.

4.4 Relationship of video quality and decryption

As we discussed in the former sections, by modulate the quantization scale in the encoding stage, we can reduce the overhead of the following three stages in the secure video communication. [Figure8] shows PSNR, execution time and energy consumption when decoding and decryption where IP ratio set to be 10, fast search, CFB mode, 256 bit key size. When quantization scale goes 1 to 4,

energy consumption reducing range is much bigger than other range. That is, modulating quantization scale 1 to 4 is more efficient than other modulations on execution time and energy consumption over the video quality. However, drastic modulation of quantization scale causes dramatic degradation of video quality as we discussed. Dropping PSNR means the visual degradation, so moderate control of quantization scale would be needed.

Those effects may be emerging only in the specific condition, but every video has the Pareto-optimal section which could minimize the degradation of video quality while maintain the optimal execution time and energy consumption. Finding the Pareto-optimal section for each video sequence is meaningful work because the limitation of energy resources.



Quantization scale	1	4	8	12	20	31
PSNR (dB)	45.9	39.1	35.3	33.2	30.8	29

[Figure 8] Relationship of video quality, decoder, and decryption

Chapter5

Conclusions

Diverse sectors make use of the application utilizing video information that emerges as the mobile embedded device is increasing. Therefore, the necessity for secure applications use the video information that includes private information, corporate or state secret is needed. However, it is obvious that there is overhead in the perspective of function and energy consumption when the general video communication is combined with security module. We confirmed that we urgently need the way to minimize the energy consumption and performance degradation maintaining video quality and security degree by handling these overhead properly. Although there are two kinds of encryption, full encryption which encrypt the entire video information and selective encryption that encrypt only the important information partly, we have done experiment using full encryption method in accordance with the experimental conclusion that the ratio of encryption is negligible in the process of encoding.

In this thesis, we estimated video quality, energy consumption and execution time by controlling various parameter, quantization scale, IP ratio, motion estimation method in the encoding and decoding stage, and mode of AES and key

size in encryption and decryption stage. As a result, we could ascertain that overhead is an enormous task considering each stage is mobile embedded device and examine the relationship between video quality and execution time or energy consumption. We learned that even though computation for encoding takes the greatest proportion, reducing the size of video information after encoding decrease overhead in the rest of process. Especially, necessary time and energy for decryption account for large part compared with those for decoding. This means that execution time and energy consumption for decryption calculation is considerable in process of decoding and lessening that decrease the overhead of receiving side that is different from the previous research that the encryption overhead takes less than encoding process. Also we found that changing the section between quantization scales is the most effective way to reducing the energy consumption for decryption. However, we should consider that increasing the quantization scale degrades the video quality. Through this result, we forged the experimental environment to suggest the better way for users to use secure video communication

We are now studying estimation methods that show the security level of video after encryption, and trying to find more efficient way for secure video communication considering not only the video quality, execution time and energy consumption, but also secure video communication. For example, when the video application for secure video communication places emphasis on security, it should provide optimal quality minimizing the overhead in terms of execution time for

implement or energy consumption when it achieves particular level of security. Moreover, we plan to investigate selective encryptions which encrypt only significant data such as header information rather than the entire compressed image.

Bibliography

[1] Jim Loney in Baghdad and David Alexander and Arshad Mohammed in Washington; editing by Myra MacDonald and Mohammad Zargham. 2010. U.S. military holds soldier in classified video leak. http://www.reuters.com/article/2010/06/07/us-iraq-usa-journalists-idUSTRE6564AR20100607

[2] Fuwen Liu and Hartmut Koenig. 2010. A survey of video encryption algorithms. Computers & Security, Volume 29, Issue 1, Pages 3--15.

[3] Changgui Shi and Bharat Bhargava. 1998. A fast MPEG video encryption algorithm. Multimedia '98,

[4] Chung-Ping Wu and Chung-Ping Wu. 2005. Design of Integrated Multimedia Compressionand Encryption Systems. IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 7, NO. 5

[5] ITU-T SG11. "H.263+ public domain codec (TMN3.2)", *Univerity ofBritish Columbia*, 1998.

[6] Information Technology Laboratory (National Institute of Standards and Technology)."Announcing the advanced encryption standard (AES)",*Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology*, 2001.

[7] Shivajit Mohapatra, Radu Cornea, Hyunok Oh, Kyoungwoo Lee, Minyoung Kim, NikilDutt, Rajesh Gupta, Alex Nicolau, SandeepShukla, and NaliniVenkatasubramanian. 2005. A Cross-Layer Approach for Power-Performance Optimization in Distributed Mobile Systems. In *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 10 - Volume 11* (IPDPS '05), Vol. 11.

[8] R.L. Rivest, A. Shamir, and L. Adleman. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), 1978, pages 120-126

[9] Information Technology Laboratory (National Institute of Standards and Technology), " Digital Signature Standard (DSS)", *Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology*, 2009

[10] Patroklos G. Argyroudis, Raja Verma, Hitesh Tewari, and DonalO'Mahony. 2004. Performance Analysis of Cryptographic Protocols on Handheld Devices. In *Proceedings of the Network Computing and Applications, Third IEEE International Symposium* (NCA '04).

[11] Nachiketh R. Potlapally, Srivaths Ravi, AnandRaghunathan, and Niraj K. Jha. 2003. Analyzing the energy consumption of security protocols. In *Proceedings of the 2003 International Symposium on Low Power Electronics and Design* (ISLPED '03).

[12] UjwalaPotdar, K. T. Talele, and S. T. Gandhe. 2009. Comparison of MPEG video encryption algorithms. In *Proceedings of the International Conference on Advances in Computing, Communication and Control* (ICAC3 '09).

[13] Kyoungwoo Lee, NikilDutt, and Nalini Venkatasubramanian. 2005. An experimental study on energy consumption of video encryption for mobile handheld devices. *In Proceedings of International Conference on Multimedia and Expo* (ICME ’05).

[14] YuanzhiZou, TiejunHuan, Wen Gao. 2006. H.264 Video Encryption Scheme Adaptive to DRM. In proceedings of IEEE Transactions on Consumer Electronics

[15] Zheng Liu and Xue Li. 2004. Motion Vector Encryption in Multimedia Streaming. *In Proceedings of the 10th International Multimedia Modelling Conference (MMM’04)*

[16] Shujun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, Kwok-Tung Lo. 2007. On the Design of Perceptual MPEG-Video Encryption Algorithms. IEEE Transactions on Circuit and System for Video Technology

[17] Yuan Li, Liwei Liang, Zhaopin Su, Jianguo Jiang. 2005. A New Video Encryption Algorithm for H.264. *in Proceedings of International Conference on Information, Communications and Signal Processing* (ICICS ‘05)

[18] Dayong Wang , Yujie Zhou, Dandan Zhao, Jufa Mao. 2009. A partial video encryption scheme for mobile handheld devices with low power consideration. *In proceedings on International Conference on Multimedia Information Networking and Security* (MINES ’09)

[19] A.Massoudi, F.Lefebvre, C.De Vleeschouwer, B.Macq, J.-J.Quisquater. 2008. Overview on Selective Encryption of Image and Video:Challenges and Perspectives. EURASIP Journal on Information Security Volume 2008

[20] Moo-Ryong Ra, JeongyeupPaek, Abhishek B. Sharma, Ramesh Govindan, Martin H. Krieger, and Michael J. Neely. 2010. Energy-delay tradeoffs in smartphone applications. *In Proceedings of the 8th international conference on Mobile systems, applications, and services* (MobiSys '10).

[21] Lide Zhang, BirjodhTiwana, ZhiyunQian, Zhaoguang Wang, Robert P. Dick, Zhuoqing Morley Mao, and Lei Yang. 2010. Accurate online power estimation and automatic battery behavior based power model generation for smartphones. *In Proceedings of the eighth IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis* (CODES/ISSS '10).

감사의 글

먼저 많이 부족한 저를 물심양면으로 도와주시고 이끌어주신 이경우 교수님께 감사 드립니다. 교수님께는 학술적인 면뿐만 아니라 인간적인 부분에 있어서도 정말 많은 것을 배울 수 있었습니다. 2년간 교수님께 배울 수 있었던 시간은 제게는 정말 큰 행운이었습니다. 앞으로 저의 앞날에 있어서도 교수님의 가르침을 잊지 않고 명심하며 살아가겠습니다. 교수님은 제게 있어서 최고의 멘토이셨습니다. 자주자주 찾아 뵙고 인사 드리겠습니다.

Professor Bernd Burgstaller and Seon Joo Kim attended the work of this thesis. I am very grateful y thank you for taking precious time for my work.

더 공부를 하고 싶다는 저의 욕심으로 집안에 도움이 되기 보다는 부담만을 드렸던 것 같습니다. 제가 끝까지 공부를 할 수 있도록 물질적인 도움과 정신적인 도움을 주신 부모님께 이루 말할 수 없이 감사 드립니다. 이제부터라도 배운 지식들을 활용해서 그 은혜를

조금이나마 갚아나가고 싶습니다. 이제는 미약하게라도 집안에 도움이 되도록 하겠습니다.

제게는 까마득한 대학교 선배이자 대학원 선배이신 광용이형, 대학교 때도 멋진 선배셨지만 대학원에서도 정말 굉장하셨습니다. 하나부터 열까지 모르는 것 투성이인 제게 이것저것 조언도 해주시고 직접적인 도움도 주셨던 형께는 정말 많은 신세를 졌습니다. 제게 있어서 형은 언젠가는 꼭 닮고 싶은 최고의 롤모델 입니다. 지금까지 그래왔듯 형은 계속해서 승승장구 하시며 멋지게 학업 이어나가실 것이라 믿어 의심치 않습니다.

학부 동기이자 대학원까지 함께 같이 입학한 승희형, 때로는 친구처럼 때로는 형으로써 항상 의지가 되었습니다. 형은 힘든 일이 생기면 제일 먼저 달려가서 상담 받고 털어놓을 수 있는 제일 편한 친구였습니다. 이제는 제가 졸업하고 형은 계속해서 학업을 이어나가게 되어 지금만큼은 자주 볼 수 없게 된다는 점이 정말 아쉽습니다. 제가

자주 놀러 올게요. 제가 형을 한박사라고 부를 날이 기다려집니다.

우리 연구실 친구들, 나이가 들어 만난 친구들인데도 마음이 잘 맞는 좋은 친구들이었습니다. 연구실의 맏형으로 항상 어린 동생들 챙기느라 고생한 지훈이형, 형이랑은 연구실 첫 학생으로써 같이 아는 것 없어 같이 고생했던 기억이 엊그제 같습니다. 지금처럼 앞으로 하는 일 모두 다 잘 해내리라고 믿습니다. 최고의 퍼포먼스를 자랑하는 요한아, 너한테는 동갑인데도 배울 점이 참 많았다. 앞으로도 지금 기세를 이어나가리라 믿는다. 항상 유쾌하고 재미있는 준형아, 그 모습 잃지 말고 지금처럼 연구실의 분위기를 밝게 만들어주길 바란다. 천재 영빈아, 나는 정말 너의 그 능력과 명석한 두뇌가 부러웠다. 내가 말 하지 않아도 잘 하리라 믿는다. 연구실의 막내 준현아, 빠른 시간 안에 연구실에 적응하고 능력 발휘 하는 모습을 보고 감탄했다. 막내자리가 힘들겠지만 조금만 참으렴. 지금처럼 의젓한 모습 잃지 말길 바란다.

내 사랑스러운 여자친구 수민아, 부족한 남자친구 만나서 정말 많이

고생했지? 오빠가 되어서 나는 네게 항상 도움만 받았던 것 같다. 네게는 정말 미안하고 고마워. 너는 정말 Amazing한 사람이야! 미국에 가서도 지금처럼 멋지게 공부하고 성공한 류박사가 되길! 다시 만날 날의 너의 모습이 기대된다.

지면상 적지 못한 많은 사람들에게도 정말 큰 도움을 받았습니다. 대학원 선배이자 이제 전문연구요원 선배인 정식이, 우리 학부 동기 맏형 동하형, 엄청나게 의지되는 순정이형, 재미있는 제이누, 건희 둘, 미정이, 태환이형, 근환이형, 승용이 등등 항상 고맙고 지금 같은 우정 변치 말자!

마지막으로 언제나 저의 버팀목으로써 항상 지켜봐 주시고 응원해주시는 할머니, 할아버지 정말 감사 드립니다. 이제 정말로 효도하고 싶습니다.