Jurnal Sarjana Institut Teknologi Bandung bidang Teknik Elektro dan Informatika
Vol. 1, No. 2 Juli 2012

Selective Encryption Algorithm Implementation for Video Call on Skype Client

Alwi Alfiansyah Ramdan[1], Rinaldi Munir[2]

[1]*Informatics Engineering, Bandung Institute of Technology*
[2]*Informatics Research Group, Bandung Institute of Technology*
Jl. Ganeca 10, Bandung, Indonesia
[1]alfiansyah.ramdan@gmail.com
[2]rinaldi-m@stei.itb.ac.id

Abstract—**Video calling is one of the widely used method of communicating. Encryption is applied to video call data to keep it secret. Real-time encryption is needed to support real-time communication such as video calling. Selective encryption is present as a solution to this problem. Skype is software that supports video calling. It cannot be ascertained whether Skype communication channel can be eavesdropped or not, since Skype communication protocol is very closed and concealed. Because of skype closed and concealed communication protocol, there is possibility that Skype party can eavesdrop communication in its communication channel. In this paper, we proposed a Skype client application made especially for video calling. Its main objective is to implement a selective encryption algorithm in video calling, especially via Skype. This Skype client is implemented in C++ programming language using Skypekit API from Skype. Testing proved that Skype client built support video calling with minor delay. Selective encryption algorithm is implemented to encrypt video in this Skype client.**

Keywords— **selective encryption, Skype client, video call.**

I. INTRODUCTION

Information is a primary needs in this era. Information can be obtained through communication. Video call is technology that is used as a medium of communication. Video calling enables two or more parties to communicate face to face even though the distance between the communicant is huge[8]. With this video call technology, distance and time problems in communication can be solved. However, there is another problem: the problem of security. This problem of security includes issues of confidentiality and the rights of access to information. There must be a mechanism that can be trusted to maintain the confidentiality of such information. The trick is to encrypt the sent information[4]. The standard encryption algorithm continues to grow. Currently, the standard encryption algorithm is AES[5].

In the use of video call, the encryption performed must support sending and receiving video call data quickly, so it does not interfere with the video call itself that is expected to occur in real-time (or close to)[7]. Selective encryption algorithm is algorithm that can support this real-time encryption. Selective encryption algorithm is a technique to encrypt compressed data file by simply doing the encryption on some part of data file and left the rest without encrypted[1].

Some examples of selective encryption algorithms are Real-time Video Encryption Algorithm (RVEA), Chaos-based Video Encryption Algorithm (CbVEA) and AEGIS. RVEA encrypts only the sign bits of I-Frames[3]. CbVEA encrypts only certain parts in accordance with the chaotic map[7]. AEGIS encrypt only the I-Frames and sequence header containing all encoding initialization parameters[9].

Skype is one example of software that supports video call. Skype is a software that allows users to communicate with each other using video chat, voice chat, or text chat via internet[6]. Skype claims that they have secured communication channel with encryption. The encryption used is RSA for key exchange, and Advanced Encryption Standard (AES) to encrypt transmitted information[14]. However, these secured channels' presence cannot be ascertained where and when. It happens because Skype hide and conceal their system including their communication protocol from outsiders[6].

Because of this sealed Skype systems and obscurity of encryption used by Skype, there is possibility that Skype party can eavesdrop communication in its communication channels. Moreover, the Skype party cannot guarantee whether the Skype party can eavesdrop the communication in their communication channels or not[14].

In this paper, we present an implementation of selective encryption algorithm for video call on Skype client. We did some experiments to measure the processing time required to perform encryption/decryption process.

II. MPEG-4 AVC/H.264

H.264/Advance Video Coding (AVC) is a method and format of video compression standard used by the industry from MPEG family. One important reason for the use of H.264/AVC as a standard and widespread use by the industry is the increased performance of H.264 than the previous video compression standard, MPEG-2. H.264 offers much better video compression performance than MPEG-2. H.264 allows video compression to produce much less number of bits than using MPEG-2 for the same picture quality and resolution on the video. Thus, there will be more video elements that can be stored or transmitted using H.264 format[13].

III. AES

AES is a symmetric key algorithm based on block ciphers. There are several variants of AES, including AES-128 and AES-256. AES-128 is a AES variant that uses 128-bits block length and 128-bits key length, whereas AES-256 is AES variant that uses 128-bits block length and 256-bits key length. In addition to these two variants, there are other variants, such as AES-192. AES-192 is AES variant that uses 192-bit key length. AES-192 is rarely used in comparison with AES-128 and AES-256. AES-128 has $2^{128} = 3{,}4 \times 10^{38}$ possible keys. Let's say there is a computer device that can perform and try one million keys in one millisecond, the time needed to try the whole keys is $5{,}4 \times 10^{18}$ years[11].

IV. RSA

RSA cryptographic system named after its discoverer, R. Rivest, A. Shamir, and L. Adleman. RSA is the most widely used public key cryptography system[10]. RSA provides information security and digital signatures. RSA security is based on the difficulty to perform integer factorization.

V. Selective Encryption Algorithm

Selective encryption algorithm is a technique to encrypt compressed data file by simply doing the encryption on some part of data file and left the rest without encrypted[1]. This is the strategy where a small portion of the encrypted bits can cause great damage to the entire file. Rather than encrypt the entire data file bit by bit, only bit with high sensitivity are selected for encryption. Furthermore, selective encryption reduces the total effort to encrypt and save more system resources. Examples of selective encryption algorithm on the video are RVEA and CbVEA.

A. RVEA

RVEA is selective encryption algorithm that only operates on sign bits of DCT coefficients and motion vectors from MPEG video. Basically, the process of RVEA is similar to VEA[12], its predecessor video encryption algorithm. VEA works on the whole I-Frame, while RVEA only works on some part of I-Frame. RVEA can use any secret key cryptographic algorithms, such as AES, as encryption function E to encrypt selected sign bits. This algorithm speeds up the encryption process by encrypting only certain sign bits in the MPEG stream. Also, it can be said that RVEA has better security endurance than VEA[3].

B. CbVEA

CbVEA is inspired by the chaos-based image encryption that change motion vector using XOR and XNOR operations with two chaotic sequences built separately and controlled by two keys that heve been determined[7]. CbVEA only operates on bits that have been selected using pseudo-random bits sequences (PRBS). This PRBS have been built by determined key.

VI. Skype

Skype is a software that allows users to communicate with each other in real-time using VoIP (Voice over IP), video chat, or text chat. Skype protocol is a proprietary internet telephony network based on peer-to-peer architecture Skype used. Skype protocol specifications is not published, and official applications using Skype protocol are closed-source[6].

Skype claims that they have secured communication channel with encryption. Encryption process cannot be removed and cannot be seen from the user side. Skype admitted using RSA for key exchange, and AES to encrypt transmitted information. But it is said that the Skype party cannot guarantee whether the Skype party can eavesdrop the communication in their communication channels or not[14].

VII. Design and Implementation

Broadly speaking, there are two processes in the implementation, the process of selecting a selective encryption algorithm and software development process that uses chosen selective encryption algorithm to be implemented on video call. The built software is called Skype-SeVid. Skype-SeVid is Skype client dedicated only for video calling that implements selective encryption algorithm to encrypt transmitted data. So that another Skype client features, such as instant messaging and file transfer, are not implemented.

Generally, the built component for selecting algorithm is a simple video encryption program implementing RVEA and CbVEA. This simple program is separated component from Skype-SeVid. The program will receive two inputs, they are the name of video input file and algorithm that will be used (RVEA or CbVEA). Video file will be encoded to the H.264 format, then the program will encrypt the encoded video file using the algorithm specified, measure encryption processing time, and then store the encryption result into the output file. This simple program flow diagram is shown in Fig. 1.

Whereas, the components of Skype-SeVid system are Skypekit Runtime, VideoHost and Skypekit UI . These Skype-SeVid components are interrelated to each other. The linkages of these components can be seen in Fig. 2. Skype-SeVid main interface is shown in Fig.3.

Skypekit Runtime is a component that regulates all forms of protocols used by Skype. Protocol specifications used by Skype are unpublished and confidential. Therefore, Skypekit Runtime is a component that can be likened to a black box. Software developers are not able to open, view, study its contents and change its functionality.

VideoHost is a component that can be used to access video data stream from Skypekit Runtime using SkypeVideoRTPInterface to get the video data stream and SkypeVideoRTPCallbackInterface to transmit video data stream back to Skypekit Runtime. With these two interfaces of Skypekit Runtime, VideoHost can manipulate the obtained video data stream. After getting video data stream from Skypekit Runtime, VideoHost will perform the encryption and decryption of this video data stream, and then will send the result back to Skypekit Runtime.

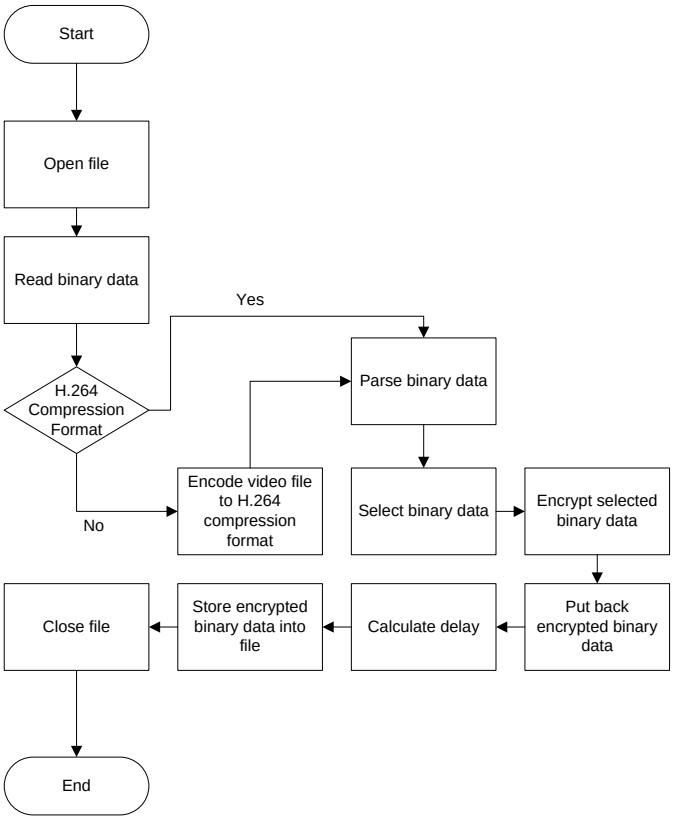


Fig. 1 Algorithm selection program flow diagram

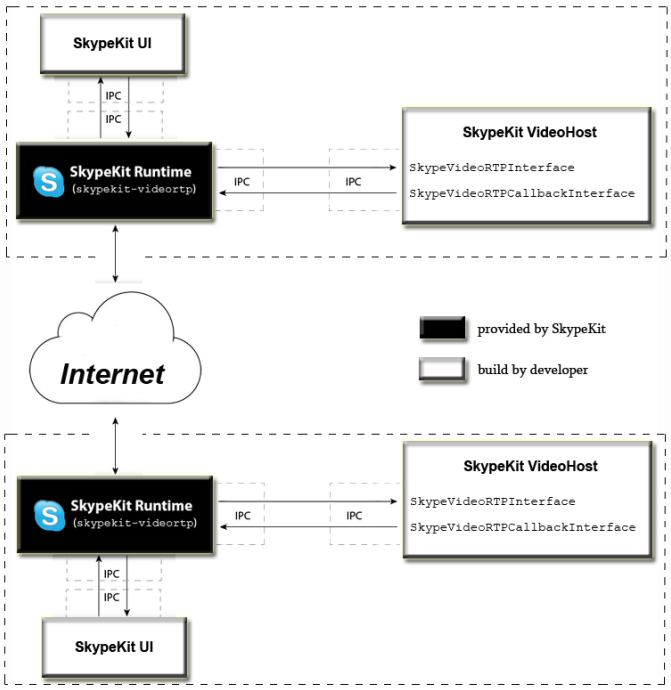


Fig. 2 The linkages of Skype-SeVid components

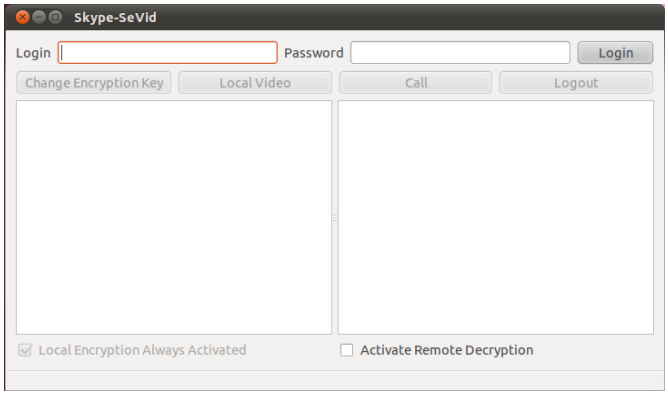


Fig. 3 Skype-SeVid main interface

Skypekit UI is a component that will be the interface between the user and Skypekit Runtime. Skypekit UI will receive input from user in form of a command to perform an action, send specific-related command to Skypekit Runtime and receive result of the command from Skypekit Runtime to be shown to user. Moreover, Skypekit UI also will arrange a secret key exchange mechanism for encryption and decryption processes taking place in VideoHost. Key exchange will be performed automatically using RSA when Skypekit UI received command to make video call.

VIII. EXPERIMENTAL RESULTS

In general, the test will be devided into two parts, the selection algorithm program test and Skype-SeVid test.

A. The Algorithm Selection Program Test

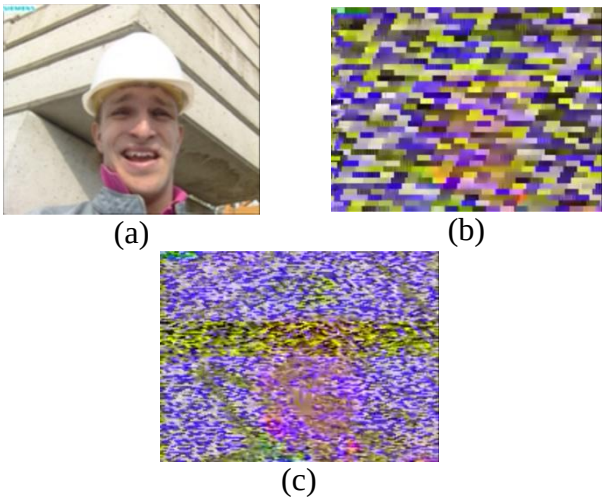
The algorithm selection program test is testing conducted to determine which candidate algorithm that will be implemented in Skype-SeVid. In this test, eight video files will be used as input for simple program. The result of processing time measurement for encryption process on eight files using RVEA can be seen in Table I. Whereas, the result of processing time measurement for encryption process on eight files using CbVEA can be seen in Table II. Encryption results using RVEA and CbVEA can be seen in Fig. 4. Summary of results of the average processing time per frame measurement for each algorithm on this test can be seen in Table III.

TABLE I.
RESULT OF PROCESSING TIME MEASUREMENT USING RVEA

File Name Input	Number of Frames	Processing Time (seconds)
bus.y4m	150	1.085
carphone.y4m	382	5.465
coastguard.y4m	300	4.314
container.y4m	300	4.254
foreman.y4m	300	4.294
grandma.y4m	870	12.303
miss_am.y4m	150	2.175
phamplet.y4m	300	4.264

TABLE II.
RESULT OF PROCESSING TIME MEASUREMENT USING CBVEA

Input File Name	Number of Frames	Processing Time (seconds)
bus.y4m	150	1.137
carphone.y4m	382	5.730
coastguard.y4m	300	4.469
container.y4m	300	4.473
foreman.y4m	300	4.480
grandma.y4m	870	13.075
miss_am.y4m	150	2.261
phamplet.y4m	300	4.523



(a) (b) (c)

Fig. 4 Experiments on foreman.y4m sequence: (a) the original image, (b) the corresponding encrypted image using RVEA, (c) the corresponding encrypted image using CbVEA

TABLE III.
SUMMARY OF THE AVERAGE PROCESSING TIME PER FRAME

Algorithm Name	Average Processing Time per Frame (milliseconds/frame)
RVEA	13.864
CbVEA	14.458

B. The Skype-SeVid Test

Skype-SeVid test is testing done to see if the application meets the expected requirements, such as the functional and non-functional needs, to see if video data stream sent to the network have been encrypted and to measure processing time for encryption and decryption processes performed. This test performed on the internet connection with data transfer speeds between 79 kbps – 145 kbps and memory usage between 912 – 1247 MB of RAM of 2048 MB of RAM.

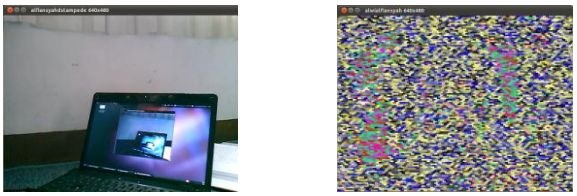
On functional and non-functional test, Skype-SeVid meets all functional and non-functional needs, whereas on encrypted data transmission test, Skype-SeVid does not meet the requirement because the sent video data stream do not have similarity with encrypted video data stream. The result of processing time measurement for encryption process on Skype-SeVid can be seen in Table IV. Whereas The result of processing time measurement for decryption process on Skype-SeVid can be seen in Table V. Encryption results on Skype-SeVid can be seen in Fig. 5. Summary of results of the average processing time per frame measurements on Skype-SeVid can be seen in Table VI.

TABLE IV.
PROCESSING TIME FOR ENCRYPTION PROCESS ON SKYPE-SEVID

Number of Encrypted Frames	Processing Time (second)	Processing Time per Frame (seconds/frame)
852	13.564	0.01592
892	15.985	0.01792
716	9.239	0.01290
991	16.103	0.01625
720	10.567	0.01468

TABLE V.
PROCESSING TIME FOR DECRYPTION PROCESS ON SKYPE-SEVID

Number of Decrypted Frames	Processing Time (second)	Processing Time per Frame (seconds/frame)
805	13.564	0.01685
871	15.985	0.01835
706	9.239	0.01309
982	16.103	0.01640
713	10.567	0.01482



(a) (b)

Fig. 5 Encryption results on Skype-SeVid: (a) the original image, (b) the encrypted image using RVEA

TABLE VI.
SUMMARY OF THE AVERAGE PROCESSING TIME PER FRAME ON SKYPE-SEVID

Process	Average Processing Time per Frame (seconds/frame)
Encryption	0.015534
Decryption	0.015902

IX. RESULTS ANALYSIS

It can be seen in algorithm selection program test, the number of processed frames very influential on the processing time. The more processed frames, the longer the prcessing time required. In addition to number of frames, frame size in pixel units are also influential. The larger the frame size, the more the number of processed bits. It can be seen too, RVEA have an average frames processing time less than CbVEA. RVEA do the bits selection in a fixed number (64 bits for each macroblock), while CbVEA do not select bits in a fixed

number, number of its selected bits depends on PRBS formed from encryption key. There is a possibility that the number of selected bits to be encrypted in CbVEA is larger than the number of selected bits to be encrypted in RVEA, so that the CbVEA processing time is longer than RVEA processing time.

Based on Skype-SeVid encrypted data transmission test, it is found that data stream sent over the network do not have similarity to encrypted video data stream or video data stream before encryption. As mentioned before, Skype claims to have communication channels secured by encryption, although no one can verify it because of closed system of the Skype protocol. The difference between encrypted video data stream and data stream sent over the network is possible because Skype encrypts the encrypted video data stream in its communication channels. However, it does not mean that the communication channel is secure from eavesdropping by Skype party itself. By encrypting the video data stream before it is sent over the network, the possibility of eavesdropping, both by outsiders and from Skype itself, become lower.

Note that the delay in the processing time measurements regardless of the time required for the data transmitted from one Skype-SeVid to another Skype-SeVid. It can be seen in Table VI, decryption process is longer than encryption process. It is possible due to the number of decrypted frames at some intervals is less than the number of encypted frames at the same intervals. This smaller number of decrypted frames is possible due to the number of frames received is less than the number of frames sent. This is due to the process of dropping packages and the loss of data packets in the network.

Based on analysis and test results, it is proved that Skype-SeVid can be run and quite reliable in carrying out its function. The weakness of Skype-SeVid are follows. Skype-SeVid cannot be run in internet connection using proxy, Skype-SeVid does not implement the other Skype features such as instant messaging, and Skype-SeVid does not implement selection and encryption on motion vectors bits. But overall, Skype-SeVid is reliable enough to support video call feature on the Skype system.

X. Conclusion

Based on implementation, testing and analysis, there are several conclusions that can be drawn. The conclusions are as follows. Selection of selective encryption algorithm can be done by measuring the performance of each selective encryption algorithm candidate in performing processes relating to video encryption. The performance in question is the time it takes algorithm candidate to complete the encryption process. The smaller the time it takes, the better the performance. Delays produced by the encryption/decryption process using selective encryption algorithm are as follows. For each video frame, it takes only an average of 15.534 milliseconds for encryption and 15.902 milliseconds for decryption process. This delay values obtained on internet connection with data transfer speeds between 79 – 145 kbps and memory usage between 912 – 1247 MB of RAM of 2048 MB of RAM. On further research, it is recommended that the next Skype client application can be run on an internet connection using proxy, implement another Skype client features, such as instant messaging and file transfer, and implement selection and encryption on motion vectors bits. The encoding and decoding processes on Skype-SeVid is done by Skypekit Runtime, so it is advisable that the encoding and decoding processes is done by VideoHost so that VideoHost have more control over the processing of the video data stream.

References

[1] M. Abomhara, O.O. Khalifa, and O. Zakaria, "An Overview of Video Encryption Techniques", *International Journal of Computer Theory and Engineering*, **2**, pp. 103-110, 2010.

[2] S.A. Baset, and H. Schulzrinne. (2004) An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. Downloaded on 7th November 2011. [Online]. Available: http://www.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf

[3] B. Bhargava, C. Shi, and S.Y. Wang, "An efficient MPEG video encryption algorithm", *Proceedings of Seventeenth IEEE Symposium on Reliable Distributed Systems*, West Lafayette, USA, pp. 381 – 386, 1998.

[4] I. Curry. (2001) An Introduction to Cryptography and Digital Signatures. Downloaded on 7th November 2011. [Online]. Available: http://www.entrust.com/resources/pdf/cryptointro.pdf

[5] Dawood, Mansoor-uz-Zafar and Abdul Raouf Khan, "Advanced Encryption Standard", National Computer Conference, 2002.

[6] B. Hayes. (2008) Skype: A Practical Security Analysis, InfoSec Reading Room, SANS Institute. Downloaded on 7th November 2011. [Online]. Available: http://www.sans.org/reading_room/whitepapers/voip/skype-practical-security-analysis_32918

[7] H. Jian, P. Li, Z. Li, Y. Mao, and Z. Wang, "A Novel Chaos-Based Video Encryption Algorithm", *Proceedings of the 6th International FLINS Conference*, Blankenberge, Belgium, World Scientific, pp. 641-648, 2004.

[8] R. Kent, and H. Tepper. (2005) Enterprise Video Conferencing: Ready for Prime Time. Downloaded on 7th November 2011. [Online]. Available: http://www.polycom.eu/global/ documents/whitepapers/enterprise_video_conferencing_ready_for_prime_time.pdf

[9] T.B. Maples, and G.A. Spanos, "Performance Study of Selective Encryption Scheme for the Security of Networked Real-time Video", *Proceedings of the 4th International Conference on Computer and Communications*, Las Vegas, Nevada, pp. 2 – 10, 1995.

[10] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, USA: CRC Press, 1996.

[11] Rinaldi Munir. (2011) Advanced Encryption Standard (AES). Downloaded on 18th November 2011. [Online]. Available: http://www.informatika.org/~rinaldi/Kriptografi/2010-2011/Advanced%20Encryption%20Standard%20(AES).ppt

[12] K. Nahrstedt, and L. Qiao, "A new algorithm for MPEG video encryption", *Proceedings of The First International Conference on Imaging Science, Systems, and Technology (CISST'97)*, Las Vegas, Nevada, pp 21, 1997.

[13] Iain E. G. Richardson, *The H.264 advanced video compression standard 2nd Ed. Chichester*, West Sussex, United Kingdom: John Wiley & Sons, Ltd, 2010.

[14] (2011) Developer Skype Website. Downloaded on 7th November 2011. [Online]. Available: http://developer.skype.com