2016 Joint International Conference on Artificial Intelligence and Computer Engineering (AICE 2016) and
International Conference on Network and Communication Security (NCS 2016)
ISBN: 978-1-60595-362-5

A Video Sensing Oriented Format-compliant Entropy Coding Encryption Scheme and Embedded Video Processing System

Chen XIAO[1,a,*], Li-Feng WANG[2,b], Qing-Lei MENG[3,c]

[1]School of CS, Beijing University of Posts and Telecommunications, Beijing, China

[2]Department of EE, Beijing Electronic Science and Technology Institute, Beijing, China

[3]Institute 706, Institute of China Aerospace Science and Industry Corporation, Beijing, China

[a]xiaochen@bupt.edu.cn, [b]lfwang@besti.edu.cn, [c]mengqinglei198029@foxmail.com

*Corresponding author

Keywords: IOT, Multimedia Sensing, Video Encryption, H.264/AVC, CABAC.

Abstract. Information security is an important issue in IOT applications such as multimedia sensing. Firstly, the study is aiming to achieve a balance between the security of massive multimedia data and the limited computation with energy resources in IOT system, while an analysis model for optimizing the protection of multimedia data is proposed. Secondly, a new lightweight format-compliant video encryption scheme is presented. By encrypting the key initial index values of the context model in CABAC entropy coding, the proposed encryption scheme achieves low complexity and could meet the real-time requirement of an unmanned aerial vehicle based video capture system. Thirdly, an embedded secure video processing system using DSP and ARM is designed, and the presented encryption scheme is implemented. Finally, the experimental results show that the encryption scheme can get a tradeoff between the efficiency and security.

Introduction

With the development of sensor communication technology and network, especially the wireless network technology, the basic technology of IOT (Internet of Things) has gradually improved. At the same time, to meet the demand of people, the concept of IOT has been extended from intelligent object connection to agricultural, industrial, education, medical care, public security, military and other fields, which attracted a great deal of interest among researchers, enterprises, organizations and even governments. And the multimedia sensing is an important application of IOT applications [1].

However, the information technology has been accompanied by information security problem from its birth. This situation is more serious in network times. And the IOT which based on the network communication technology inherits its security problem naturally. So the security issues become a central concern which could hamper the development of IOT technology, and has attracted widespread attentions [1], [2]. For this reason the European Union established a framework of privacy and data protection impact assessment of IOT applications [3]. IETF also proposed a draft on security considerations in the IP-based IOT [4].

To analyzing the security of IOT, the content of its security issues can be divided into different layers of IOT. There are several hierarchical models of IOT, in which three-layer architectures are widely accepted by researchers [5]. Although different scholars have different expressions, the above three layers can be interpreted as sensor layer, network layer and application layer in general.

Except the traditional security problems in distributed system, the unique characteristics of the IOT has brought in some new security problems like the safety of sensing devices their own, the certification of heterogeneous equipments, processing of massive multimedia data, and etc. However the limited computation and energy resources in sensor layer is the most important factor in all of the security issues, since limited resource restricts the complex encryption process operated on the massive multimedia data, and leads to seriously challenges [1].

Before the research of IOT applications, scholars do not pay a lot of attention to limited resources in devices of distributed system. However, because of the unique characteristics of unplugged device in IOT, data processing with limited resources has attracted a great deal of interest from researchers, and there have some researches on it [1], [4]. In the meantime, the impact of limited resources on IOT security has also been considered by scholars. How to achieve data confidentiality under tight resource constraints has become an important topic. In IETF's draft of "Security Considerations in the IP-based IOT", the first challenge of IOT security is the "tight resource constraints". [6]And some other researches pointed out that complex security process should not be used, and energy-efficiency schemes should be considered to achieve a balance between performance and security. Those researches also indicate that the existing study on data confidentiality under tight resource constraints is relatively unsubstantial.

In recent years, video encryption schemes for massive multimedia data have been researched [7]. Those schemes always focus on the real-time character, and the cost of energy and other resources is generally disregarded. In addition, [8] points out there is no scheme that fits for all applications. The selection of an appropriate algorithm should depend on the particular application requirements. Until now experimental research on data confidentiality under limited resource is relatively rare.

In the following sections, an analysis model for optimizing multimedia data encryption is proposed to balance the dissymmetry between the massive multimedia data and the limited computation with energy resources in IOT; secondly, a lightweight format-compliant video encryption scheme is presented by encrypting the key initial index values of the context model in the CABAC entropy coding. Thirdly, an embedded secure video processing system using DSP and ARM is designed, and the presented encryption scheme is implemented; finally, experimental studies on the encryption scheme are given.

Application-environment Oriented Encryption Optimizing under Resource Constraints

The Trend of Resources Constraints

In the past, the shortage of encryption resources is somewhat ignored in the study of data security. However, in recent years, the growth of the volume of data to be encrypted overwhelms the growth of encryption capability, while the power resource in sensing device grows more slowly.

Firstly, the growth of processing ability of encryption is highly correlated with the growth of the CPU speed. According to Moore's Law, the performance of computer would double every 18 months, or grows about 60 percent a year [9]. Comparatively, the disk density increase 100 percent per year [9], which is faster than Moore's Law. Moreover, a lot of researchers point out that the bandwidth of core network and image process ability grows even faster than disk densities. In addition, the computation and encryption capabilities of battery-powered equipments are also constrained by battery capacity, which makes the resource-constrained problem trickier. Predicatively, the dissymmetry between the throughput of encryption algorithm and the data volume to be encrypted will aggravate. Therefore a model for data encryption is very necessary.

Optimization Model of Data Encryption under Limited Resources

When encryption resource is adequate enough to encrypt the data, for example, encrypting a big text file without time limit, traditional encryption scheme will be successful. In this case, encryption resources is allocated averagely into each symbols or bits of plain text, thus we assume all symbols are of equal importance. However, as to video sensing, encryption resource is not adequate enough. Hence the traditional encryption schemes which allocate the encryption resources averagely are unsuitable. Moreover the distribution of information utility value in the media data is not average. Considering the limited encryption resource, an encryption resource allocation principle, which can optimize the security of information value, is very imperative.

We use the following expression to figure the optimization principle we proposed.

$$\begin{cases}\text{min. } \mathit{valueLeak}\ (M, \mathit{MES}). \\ \text{s.t. limited resources \& real-time constraints.}\end{cases} \tag{1}$$

Where *M* is the target multimedia data, and *MES* is a Multimedia Encryption Scheme, we call it Limited Resources Optimal Utility-value Model. The optimization principle of this model is selecting appropriate encryption schemes for media data to maximize the utility value of multimedia information been protected (equals to minimize the utility value which could be got by attackers).

When *M* is a single stream, *MES* means a specifically multimedia encryption algorithm. Comparatively, when *M* is the streams in a system, *MES* means a whole scheme include the selection of encryption algorithms and selection of streams to be encrypted. It should determine the optimum encryption algorithm for each stream in the system, and let the encryption resources be used concentrated on the streams with higher security weightiness.

Design of Encryption Scheme in a Specific Environment

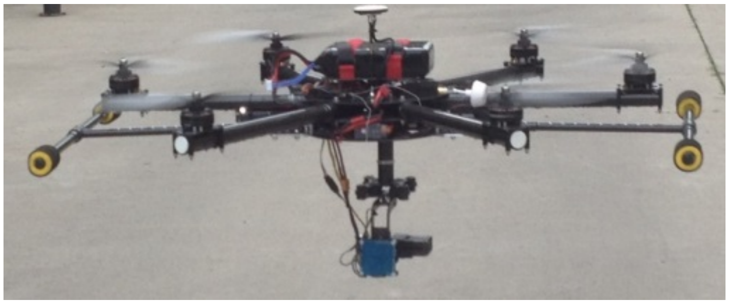


Figure 1. The Application Background of Our Encryption Scheme is a Video Capture System Based on a Multi-axis Unmanned Aerial Vehicle.

Because the utility value of multimedia information in the proposed optimization model is closely related to the application environment, the optimization strategies should link with the application environment closely. The application background of our encryption algorithm is a video capture system based on a multi-axis unmanned aerial vehicle, which is shown in Fig. 1. In this application the commercial value of video should be protected. Since the unmanned aerial vehicle is powered by batteries, the energy resource in our system is very valuable, and directly affects the vehicle's durability. The encryption scheme proposed in the next section will focus on the application environment given above.

A Format-compliant Entropy Coding Encryption Scheme

The Principle for Encryption Scheme Design

In the designing of encryption strategy in an actual system, attention should be paid to characteristics and requirements of the application. Compared with the military and other sensitive applications, the protection of commercial aerial video should focus on the security of video's commercial values, limit resources, real-time constrain, while format-compliance and appropriate compression ratio are also could not be ignored.

CABAC Encoding and Encryption Scheme

CABAC (Context-based Adaptive Binary Arithmetic Coding)[10] in H.264/AVC is designed to get a better exploitation of the characteristics of non-zero parameters as compared to CAVLC. It is a little more complex, but can offer about 10% better compression rate than CAVLC on average.

As is shown in Fig.2, CABAC mainly consists of the following stages. Firstly, binarization converts nonbinary syntax elements to binary numbers. However, if a binary syntax element is given, this step should be skipped over. For each element of the binary string, regular or bypass coding mode should be chosen. In the regular coding mode, the given binary string firstly enters the context modeler and a context model is selected. Then, the binary value along with its model is passed to the regular coding engine. On the other hand, bypass coding is used to skip over the context modeling.

After analyzing, some important initial index values in the context model of CABAC entropy coding is selected to be encrypt. In this subsection, the details will be given.

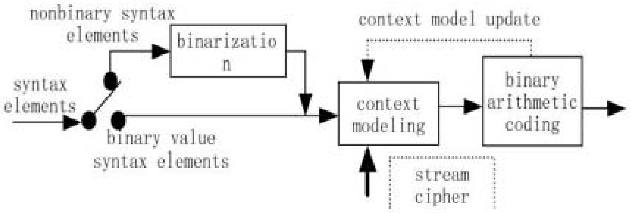


Figure 2. The CABAC Encoder.

Firstly, in the binarization stage (the first stage on the left of Fig.2.), different binary encoding schemes are used to deal with different encoding elements. The coded information includes sign information and texture information. As to sign information, it is not suitable for encryption, since the encryption will change the format information and also could not get enough security. On the other hand, the texture information contains the most volume of the video data, and the information value distribution is relative even. If all texture information is encrypted, the encryption scheme will degrade to traditional fully encryption. Based on the above two reasons, it is not suitable to implement the encryption in the binarization coding step.

Secondly, in the stage of arithmetic encoding (the third stage on the right of Fig.2.), each binary syntax elements is encoded according to the selected probability model. CABAC achieves good compression performance through selecting probability models for each syntax element according to the element's context, and adapting probability estimates based on local statistics using looking up tables instead of multiplication operation. The tables are designed to produce shorter codeword for more frequently-occurring values and longer codeword for less common values. If the context adaptive model and the probability values are encrypted, it is bound to bring down the compression ratio, and reduced the efficiency of CABAC dramatically. So it is not advisable.

Finally, in the context modeling stage, a model probability distribution is assigned to the given symbols, which drives the actual coding engine to generate a sequence of bits as a coded representation of the symbols according to the model distribution. There are 399 context probability models in H.264/AVC standard, and each context model has an index value. The probability model depends on the statistical results tremendously, and is kept update during the encoding process. If the encryption scheme disrupts the probability models directly, it will change the statistical characteristics, and bring down the compression ratio significantly. So disrupting the context models is meaningless.

From the above analysis of the entropy coding process of the H.264/AVC encoder, particular attention should be paid to encrypting the initial index value of the context model. Encrypting it would not influence the compression ratio a lot, in addition its size is so small but has a notable information value. Encrypting the initial index value could distribut the context model. So if the attackers do not acquire right initial index values, the encrypted video is unintelligible.

The Encryption Design in Context Modeling

By analyzing the key parameter in the encoder process, it could be found that the main information of I/SI frame is the coded block flag (CBF) and the coded block pattern (CBP), and the key information of P/SP and B frame is the motion vector difference (MVD) in horizontal and vertical directions. On the one hand, if only the index of probability models of the CBP and CBF elements are scrambling, video motion information are still in plaintext, which would lead to a leak of important video information [11]. On the other hand, if just encrypt the index of probability models of the MVD, the main information in I frame would be vulnerable. At last the initial indexes of probability models of CBF, CBP and MVD is selected to be encrypted in our video encryption scheme.

Since the selected data are binary bit stream, to achieve the format compliance,stream cipher should be used. The main types of stream cipher include RC4, A5, SEAL, chaos cipher, and so on. Because it has been widely discussed, RC4 is used in the following embedded system.

An Embedded Secure Video Processing System

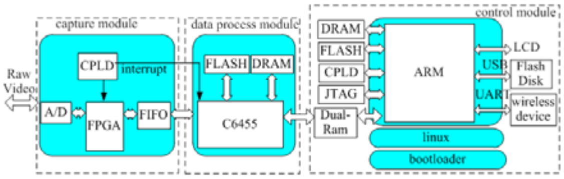


Figure 3. An Embedded Secure Video Processing System Using DSP and ARM9.

An embedded video processing system using DSP and ARM9 is designed, and the encryption scheme proposed in section III is implemented.

The hardware platform can be divided into three modules, and the architecture is shown in Fig. 3. It includes the video capture module, the data processing module and the control module.

Video Capture Module

The capture module consists of A/D (analogue to digital converter), FPGA and FIFO. When control commands are given by CPLD at runtime, FPGA will parse the command words and process the captured data according to the user request patterns. Then FPGA can capture video signals and store them into FIFO in a given format, and inform data processing module by an interrupt signal. And then the DSP with EDMA transmit the data into the periodic buffer in DRAM. The format conversion mentioned above includes video resolution and video type, like converting 4:2:2 YUV to 4:2:0 YUV format.

Data Processing Module

The data processing module consists of DSP, DRAM and FLASH. TMS320C6455 DSP is used to perform data processing. It has a frequency of 1GHz, 2MB RAM and 8 parallel processing units. All the intermediate data of reference frames and reconstructed frames are put into the outer temporary buffer in a 64MByte DRAM. An 8MB flash memory is used to save the bootloader program. At runtime DSP can read video data from the capture module, and process them with specified H.264/AVC encoder and then transmit them to the control module. Due to the resource limitation and the complexity of encoding algorithm, the implementation of the encoder is optimized to achieve real-time processing. The optimization includes arithmetic optimization, resource optimization, transmission optimization and code-level optimization. In addition, the encryption scheme proposed in section III is implemented in this module.

Control Module

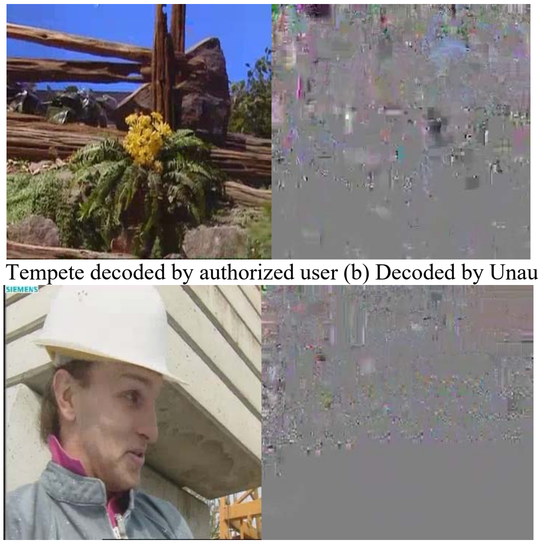
The control module is designed based on S3C2410 processor with kernel of ARM920T and embedded Linux. In this module DRAM and Flash memory are used as the memory, the CPLD is used to provide external chip select, the dual RAM is used to engage the data transmission between the DSP and ARM, JTAG port is used for debugging and testing. The control module could get the encrypted video streams from the dual RAM, and then a flash disk is used to store the streams. In addition, the snapshot of video could be send to remote control unit by wireless channel in future expansion.

Experimental Results and Performance Analysis

Although low complexity is one of the most important principles of designing video encryption scheme, the time increasing in the compression process can be ignored. That is because the RC4 encryption algorithm could get a speed of more than 200MBps. In addition, the ratio of data selected to be encrypted is excessively small. So in this section we focus on the visual security and compression ratio.

Video Security

In order to analyze the performance of the proposed encrypting scheme, several standard sequences are tested. The results of News and Tempete are shown in Fig. 4. Since the encryption scheme is format compliant, the bit stream can be decompressed by most standard decoder, but only authorized legitimate users could decrypt the streams properly, and get a readable video. Fig. 4 (a) and (c) show the visual results decoded by the authorized users, and Fig. 4 (b) and (d) show results of the unauthorized users.



(a) Encrypted Tempete decoded by authorized user (b) Decoded by Unauthorized User

(c) Encrypted Foreman Decoded by Authorized User (d) Decoded by Unauthorized User

Figure 4. Comparison of Video Decoded by Authorized and Unauthorized User.

Compression Ratio

Table 1 compares the encrypted bitrates of several video sequences with the unencrypted ones. Results show that proposed encryption scheme does not make notable influence on compression ratio.

Table 1. Comparison of the Size of Unencrypted and Encrypted Video Sequences.

Sequence	Frame number	unencrypted File (KB)	Encrypted file (KB)	Compression ratio increasing
foreman	300	465,057	465,668	0.131%
news	300	465,629	466,151	0.112%
mobile	300	478,032	478,513	0.100%
tempete	300	424,418	424,670	0.059%

Conclusion

Information security is an important issue in IOT applications such as multimedia sensing. Firstly, an analysis model for optimizing multimedia data encryption is proposed. It achieves a balance between the security of massive multimedia data and the limited computation with energy resources in IOT. Secondly, a new lightweight format-compliant video encryption scheme is presented by encrypting the key initial index values of the context model in the CABAC entropy coding. It can meet the application requirements of the given video capture system. Thirdly, an embedded secure video processing system using DSP and ARM is designed, and the presented encryption scheme is implemented. Finally, the experimental results show that the encryption scheme can get a tradeoff between the efficiency and security, and has format-compliance, low encryption complexity, appropriate compression ratio and visual security.

Acknowledge

We acknowledge the support of the National Natural Science Foundation of China (No.61300182).

References

[1]Atzori, L., Iera, A., & Morabito, G.: The internet of things: A survey. Computer Networks, 54(15), 2787-2805 (2010).

[2]Chen, X., Makki, K., Yen, K., & Pissinou, N.: Sensor network security: a survey. Communications Surveys & Tutorials, IEEE, 11(2), 52-73 (2009).

[3]Privacy and Data Protection Impact Assessment Framework for RFID Applications, http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf.

[4]Garcia-Morchon, O., Keoh, S., Kumar, S., Hummen, R., Aachen, RWTH., Struik, R.: Security Considerations in the IP-based Internet of Things. IETF Internet Draft, (2012), http://tools.ietf.org/html/draft-garcia-core-security-04.

[5]Ning, H., & Liu, H.: Cyber-Physical-Social Based Security Architecture for Future Internet of Things. Advanced in Internet of Things, 2(1), 1-7 (2012).

[6]Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S.S., Wehrle, K.. Security Challenges in the IP-based Internet of Things. Wireless Personal Communications, 61(3), 527-542.

[7]Lian, S.: Multimedia content encryption: techniques and applications. CRC Press, Boca Raton, FL, USA (2008).

[8]Liu, F., & Koenig, H. A survey of video encryption algorithms. computers & security, 29(1), 3-15.

[9]Gray, J., Patterson, D.: A conversation with Jim Gray. ACM Queue, 1(4), 53-56(2003).

[10]Marpe, D., Schwarz, H., & Wiegand, T.: Context-based adaptive binary arithmetic coding in the H. 264/AVC video compression standard. Circuits and Systems for Video Technology, IEEE Transactions on, 13(7), 620-636(2003).

[11]Agi, I., & Gong, L.: An empirical study of secure MPEG video transmissions. Proceedings of the Symposium on Network and Distributed System Security, 1996., pp. 137-144. IEEE. (1996).