About an image encryption solution adapted for surveillance flying systems

Ciprian Răcuciu, Nicolae Jula, Cosmin Adomnicăi

Abstract—This paper presents an encryption system developed to be used on an Electrical Accelerated mini-helicopter. The helicopter was developed for monitoring and surveillance purposes. The hart of the encryption system is the CV700C motherboard and it's VIA C7 microprocessor with ultra low power consumption and efficient heat dissipation. The whole system is composed from two systems and six modules: image capture, encryption, two radio link modules, decryption and display module. The first three modules are implemented on airborne system and the last three modules on the base station system. The airborne hardware platform is the CV700C motherboard and the base station is an Intel microprocessor based notebook. For encryption, Rijndael algorithm was used.

***Keywords*—**Encryption, Rijndael, DirectShow, Wireless, Embedded

I. Introduction

An UAV[1] is an airborne system, without a pilot, which flies by means of a remote control or by using an autopilot installed on board and carries sensors or weapons. It can be used only once or reused many times. Comparing an UAV with a classical airplane, most of the times, the UAV is small and light and the load is composed from sensors used in reconnaissance and surveillance missions, or in target acquisition missions. Now, there are new mission for UAV, like combat, intelligence, and civil applications [8]. Because any transmission from a military UAV must be secured it's a must to use an encryption method to protect de confidentiality of the transmitted data. Because of the restrictions applied to weight, dimensions and power consumption of any UAV module, it was chosen the CV700C motherboard manufactured by Lex Inc. which is 200 mm long and 150 mm wide. For an increased endurance to vibrations, the hard disk was replaced with a Compact Flash memory card. To maximize the encryption speed and to reduce the footprint the Windows XP Embedded operating system was used [4, 5]. The program was written in C++ programming language using the DirectShow API[2] which has the whole support for buffering and frame dropping [1].

Manuscript received January 31, 2008. This work was supported in part by the Military Techn. Academy, Bucharest, ROMANIA; Revised March 29, 2008

Ciprian RĂCUCIU is with the Military Technical Academy, B-dul George Coşbuc 81-83, Sector 5, 050141, Bucharest, ROMANIA (e-mail: ciprian.racuciu@gmail.com).

Nicolae JULA is with the Military Technical Academy, B-dul George Coşbuc 81-83, Sector 5, 050141, Bucharest, ROMANIA (e-mail: nicolae.jula@gmail.com).

Cosmin ADOMNICĂI is with the Military Technical Academy, B-dul George Coşbuc 81-83, Sector 5, 050141, Bucharest, ROMANIA (e-mail: ado_atm@ yahoo.com).

II. The system

The system is composed of:

- Digital video camera with USB interface;
- CV700C motherboard;
- RF modules;
- Notebook.

TABLE I
WEIGHT AND PRICE OF USED COMPONENTS

Device	Weight[g]	Price[€]
CV700C	500g	320€
Gigabyte 802.11b/g	15g	20€
Canion video	20g	10€

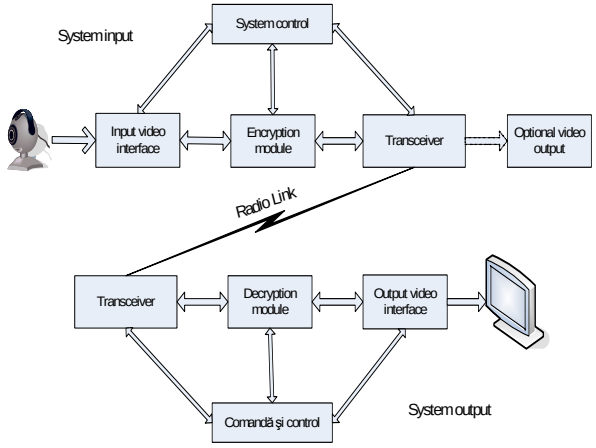

Fig. 1 The system

[1] Unmanned Aerial Vehicle

[2] Application Interface

Fig. 2 An UAV built by Professor Nicolae Jula [8]

Fig. 3 Video camera attached details

Fig. 4 Aspect of a flying UAV

The motherboard is based on VIA C7 microprocessor which operates at a frequency of 1 GHz. The microprocessor is built for applications with low power consumption requirements. On full load, the consumption of the microprocessor is 11 W and of the entire board is 25 W. To the motherboard are connected a video camera which takes pictures at a rate of 25 frames/second and a 802.11 wireless radio module which operates in the public spectrum. On this motherboard runs the airborne encryption subsystem. The other component of the system is the base station which runs on an Intel based microprocessor notebook. It receives data from the integrated 802.11 wireless module and feeds the data to the decryption module and displays the decrypted images on the monitor. The airborne encryption module can be controlled via radio link and there can be changed the encryption keys and the encryption modes.

Fig. 5 CV 700C motherboard

A. The operating system

Windows XP Embedded is a componentized form of Windows XP Professional in which the developer can choose which components to add [4, 5]. This is a big advantage because a very fast, small footprint operating system can be implemented. The distribution used had 508,33 MB in which the user interface, administration tools and installer components were included. The operating system can become even faster and smaller in the production state which does not require additional user friendly components.

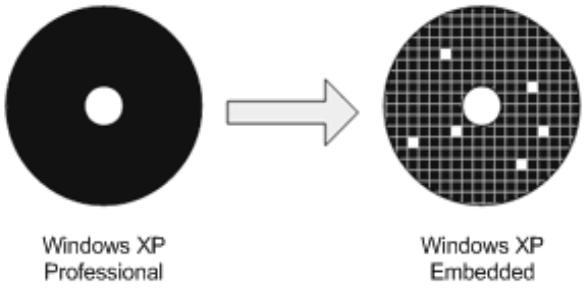

Fig. 6 Windows XP Professional vs. Windows XP Embedded

B. DirectShow API

To benefit from the full power of Windows operating system, the DirectShow framework was used [1]. Because DirectShow is a filter based framework, there were developed several filters:

- Encryption and decryption filter;
- RF interface modules (client and server);

The video input and output filters are contained in the DirectShow API. The main program initialises the filters and controls different parameters like:

- Image resolution;
- Bit depth;
- Encryption mode;
- Encryption key.

In this case, a resolution of 320x240 pixels and a bit depth of 24 bits/pixel were used. So the entire image contained 230400 bytes without the header used to pass the image parameters between filters, which added extra data [2].

C. The encryption module

The encryption module is based on the Rijndael algorithm in which the block and key size are limited at 128 bits [3]. This limitation appeared to meet the encryption speed requirements. The algorithm is composed from four major operations made to the data block [3]:

- SubBytes;
- ShiftRows;
- MixCollumns;
- AddRoundKey.

The SubBytes transformation is defined as a non-linear byte substitution which operates on the State. In SubBytes, the calculation of the multiplicative inverse can be efficiently done using a "table lookup" method: a small table of 28 = 256 pairs of bytes can be built once and used forever.

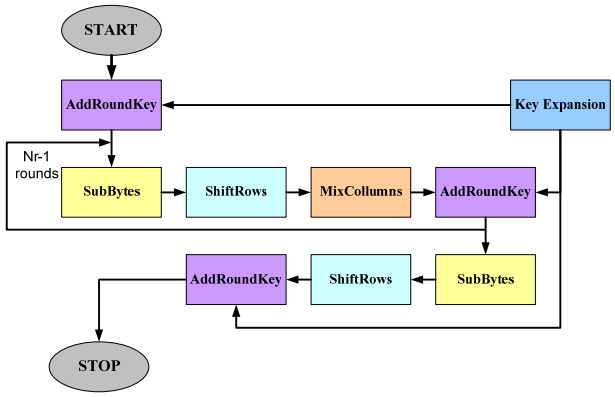

Fig. 7 Rijndael algorithm block scheme

In ShiftRows, the rows of the state are cyclically shifted over different offsets. The first row is not shifted, the second row is shifted over one byte, the third row is shifted over two bytes and, finally, the fourth row is shifted over three bytes.

The MixColumns transformation operates on the State column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo x^4+1 with the fixed polynomial: $3x^3+x^2+x+2$ [3, 7].

The AddRoundKey operation consists in the simple addition of the round key with the State. The Round Key is generated by means of the key schedule.

The algorithm uses the cipher key to generate an extended key. This key is used by the AddRoundKey operation. This entire process is called Key Schedule.

- Key Schedule consist in two components:
- Key Expansion;
- Round Key selection.

The algorithm was implemented using three modes of operation: ECB[3], CBC[4], CFB[5] [6]. In this application the ECB mode was implemented for testing purposes because of the security problems caused by the image redundancy [2]. This mode can only be used in tandem with a compression module.

D. RF Modules

The protocols used for feeding the data to the wireless device were TCP and IP in stream mode. The TCP protocol handled packet retransmission and the 802.11 RF module handled error corrections. The radio link could not be used at its full potential because of minimum delay required and the synchronization that was taking place in background.

III. Real Time Encryption Example

Fig. 8 Original image

Fig. 9 Encrypted image using ECB mode

[3] Electronic CodeBook
[4] Cipher Block Chaining
[5] Cipher FeedBack

Fig. 10 Encrypted image using CBC mode

Fig. 11 Original image

Fig. 12 Encrypted image using ECB mode

Fig. 13 Encrypted image using CBC mode

Fig. 14 Encrypted image using CFB mode

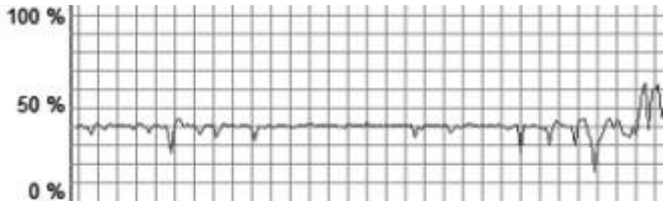

Fig. 15 Radio link load

IV. STATIC IMAGES ENCRYPTION EXAMPLES

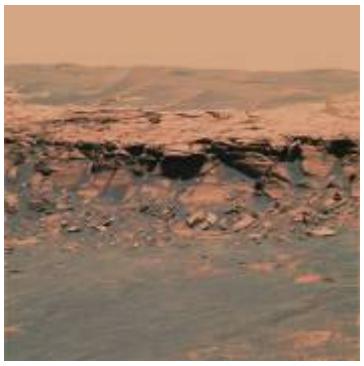

Fig. 16 Original image

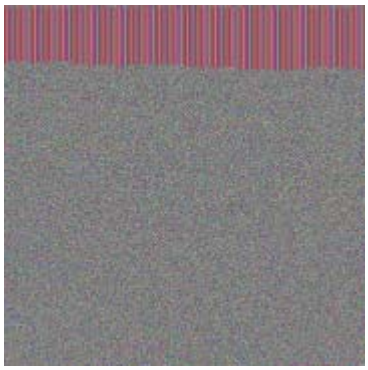

Fig. 17 Encrypted image in ECB mode

Fig. 18 Encrypted image in CBC mode

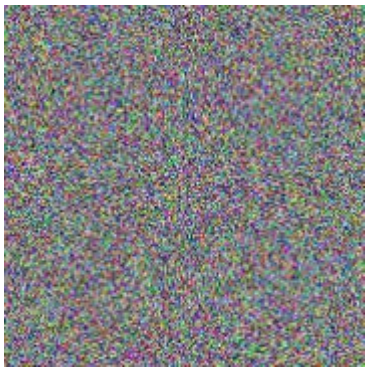

Fig. 19 Encrypted image in CFB mode

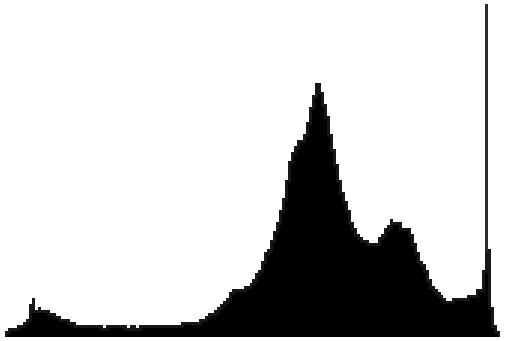

Fig. 20 Histogram of original image

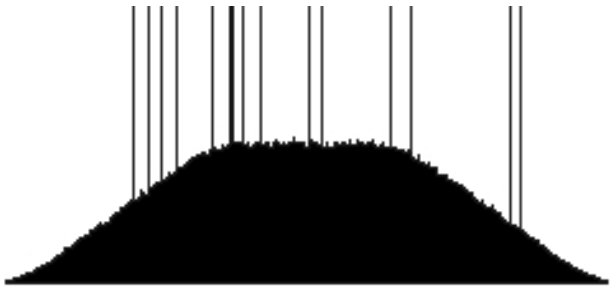

Fig. 21 Histogram of encrypted image in ECB mode

Fig. 22 Histogram of encrypted image in CBC mode

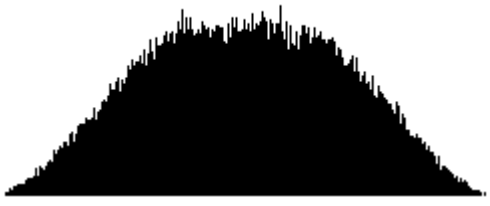

Fig. 23 Histogram of encrypted image in CFB mode

V. Conclusions

In the three modes of operation (ECB, CBC, CFB) the achieved standard deviation is between 49.36 and 49.41. From the statistical point of view de difference is very small. Although ECB mode is the fastest, there are problems in using this mode because it doesn't use the process of chaining and that is why ECB mode has problems; a continuous area of the same color has the same encrypted result. This can be resolved using an image compression module which eliminates the redundancy [9].

The key length was limited at 128 bits because of the limitations imposed by the processing power and the power consumption. Although the key is small, there are 340282366920938463463374607431768211456 possible combinations. If the key is created using a good pseudo-random generator, the key length shouldn't be a problem.

TABLE II
PERFORMANCE OF THE ENCRYPTION MODES USED

Encryption mode	Average link load	Average frames/second
ECB	39%↔2,304 Mbps	10
CBC	40%↔2,073 Mbps	9
CFB	40%↔2,073 Mbps	9

TABLE III
STANDARD DEVIATION OF THE IMAGES IN DIFFERENT ENCRYPTION MODES

Encryption mode	Std. Dev.
Original image	35,52
ECB	49,39
CBC	49,41
CFB	48,36

The histograms show that most of the values are gathered near the median.

The encryption algorithm was implemented in software and because of that the frame rate was around 10 frames / second. The VIA C7 microprocessor has a built-in hardware encryption block. The encryption process can be made in hardware at a speed around 2Gbps, leaving enough free resources for image processing tasks, like compression, object recognition, path estimation etc. Although the helicopter runs on batteries, the power consumption of the processor is small (1W in idle mode and 12 W in full load mode).

There is a background communication between the DirectShow filters. The base system can command the change of encryption modes and encryption keys of the airborne system while running, increasing the strength of the encryption system. The keys are not transmitted via radio link; instead they are built-in and can be programmed before a mission.

DirectShow's big advantage is that the video software chain is modular. In this chain other filters can be added, filters like video compression. The filter chain is constructed and controlled by the main program. If in a moment another type of video processing is needed, the entire chain can be stopped and reconstructed accordingly.

The helicopter is silent and small. It can be used in tasks where is necessary to approach the objective without being seen or heard [8]. The disadvantage is that the range is reduced in comparison with a fuel driven helicopter. Being small, it can be transported easily on the field using a small car.

References

[1] Mark D. Pesce, „Programming Microsoft DirectShow for digital video and television", Microsoft Press, 2003.
[2] Andreas Uhl, Andreeas Pommer, „Image and video encryption - From Digital Rights Management to Secured Personal Communication", Springer 2004.
[3] Joan Daemen, Vincent Rijmen – „The Design of Rijndael", Springer, 2002.
[4] Microsoft Platform SDK Help.
[5] Microsoft Windows XP Embedded Help.
[6] Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", by CRC Press, 1996.
[7] Ciprian Racuciu, ,,Lecture of Information Theory", Military Technical Academy Bucharest, 2004.
[8] Romanian Space Agency, AEROSPATIAL program, Contract no. 60/2002, "Electrical Accelerated mini-Helicopter used for monitoring".
[9] Ciprian Răcuciu, Nicolae Jula, Florin-Marius Pop, "About an adapted image compression algorithm for surveillance flying systems", International Journal Of Mathematical Models And Methods In Applied Sciences Issue 2, Volume 1, 2007, pg. 41-45, ISSN: 1790-031X.