Crypto-Compression of Medical Images by Selective Encryption of DCT

William Puech, José Marconi Rodrigues

CRYPTO-COMPRESSION OF MEDICAL IMAGES BY SELECTIVE ENCRYPTION OF DCT

W. Puech et J. M. Rodrigues.

Laboratoire LIRMM, UMR CNRS 5506, Université Montpellier II
161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE

william.puech@lirmm.fr, jose-marconi.rodrigues@lirmm.fr

ABSTRACT

The traffic of digital images has grown rapidly in the Internet. Security of image becomes important for many sectors mainly for medical applications. Nowadays, the transmission of medical images is a daily routine, especially over wireless (battlefields, traffic accidents, etc). Partial encryption is an approach to reduce the computational resources for huge volumes of multimedia data in low power network. This paper presents a method of partial or selective encryption for JPEG images. It is based on encryption of some quantified DCT coefficients in low and high frequencies. We have combined compression and encryption in order to fully dissimulate the visual information of the image and to see the image in low quality resolution.

1. INTRODUCTION

The increased popularity of multimedia applications has demanded a certain level of security. Because common encryption methods generally manipulate an entire data set, most encryption algorithms tend to make the transfer of information more costly in terms of time and sometimes bandwidth. Thus, users pay a price for security proportional to their desired level of security. One possible solution is a system of partial encryption that works cooperatively with a standard compression scheme (JPEG), encrypting only the smallest portion of the data that makes the entire data set unusable.

There is a wide spectrum of JPEG applications that demand security on a modest level. Therefore, the search for fast encryption procedures appropriated for particular environments are required. Selective encryption is a recent approach to reduce the computational requirements for huge volumes of multimedia data in distribution networks with different client device capabilities [1]. It only protects the most important parts of an image to minimize computational efforts in real-time applications.

In this work, we propose a new method of selective encryption for JPEG images. It is based in AES (Advanced Encryption Standard) cipher and DCT coefficients. In Sections 2.1 and 2.2 we introduce the main ideas, review basic terms and discuss a possible application scenario. In Section 2.3 we introduce the purposed method. In Section 3 we present and compare the results.

2. SELECTIVE ENCRYPTION OF JPEG COMPRESSED IMAGES

2.1 Previous Works

The selective encryption (SE) can match application requirements without the overhead of full encryption. However, the security of SE is always lower as compared to full encryption. So, the reasonable utilization of SE should be investigated thoroughly in order to decide whether its use is appropriated for the environment and confidentiality required [5] . The JPEG is a commonly used standard method of image compression. It is still largely employed in picture processing, security communication and industry [2]. Nowadays, this format has a huge quantity of images and hardware/firmware dedicated manufactured such as digital cameras, medical image capturing and scanners. The above cited devices already exist and it is welcome suggestions for new and fast methods to optimize JPEG format concerning the confidentiality. Several SE methods were created by other authors specially encryption of DCT based coded images. Tang [3] proposed a technique called zigzag permutation. Droogenbroec and Benedett [4] originated a technique that encrypts a selected number of AC coefficients. In their method, the DC coefficients are not ciphered because they carry important visible information and they are highly predictable. Hebert *et al* [6] have proposed a method that the data (DC and some AC coefficients of each block) are organized in a scalable bit streams form.

2.2 JPEG image

In the standard JPEG algorithm the image is decomposed in 8×8 blocks, these blocks are transformed from the spatial to the frequency domain by the Discrete Cosine Transform (DCT). Then, each DCT coefficient is divided by its corresponding constant in a standard quantization table and rounded down to the nearest integer. After this step, the DCT quantized coefficients are scanned in a predefined zigzag order to be used in the final step, the lossless compression as illustrated Figure 1.

Figure

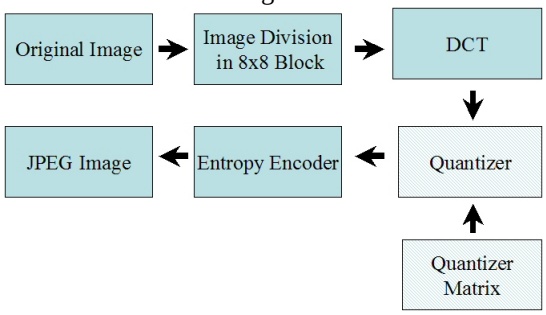

Figure 1: Compression JPEG

In each block the 64 DCT coefficients are set up from the lowest upper left corner) to the highest frequencies (lower right corner). The most important visual characteristics of the image are placed in the low frequencies while the details are situated in the higher frequencies. The HVS (Human Visual System) is most sensitive to lower frequencies than to higher ones.

2.3 The purposed Method

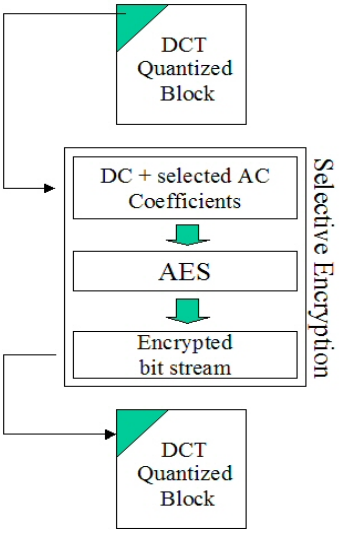

Figure 2: Plan of the purposed method

The main idea of the purposed method is to take the DC and some AC coefficients of the lowest frequencies to construct a stream of 128 bits (in our case) to use in AES (Model-1), Table 1. In the Model-2, Table 2 we work in the highest frequency coefficients. In Figure 2 we can see the global overview of the method.

The AES is nowadays the standard cipher that has replaced the DES (Data Encryption Standard). To encrypt a block of data in AES, we first perform an Add Round Key step (XORing a subkey with the block) by itself. There are regular rounds that involves four steps. First is the Byte Sub step, where each byte of the block is replaced by its substitute in an S-box. Next is the Shift Row step. Considering the block to be made up of bytes 1 to 16, these bytes are arranged in a rectangle and shifted. Next comes the Mix Column step. A matrix multiplication is performed: each column is multiplied by the matrix. The final step is Add Round Key. This simply XORs in the subkey for the current round [8].

Coefficient	Size (bits)	Range
[0,0]	11	-1024 to 1023
[1,0], [0,1]	9	-256 to 255
[2,0],[1,1],[0,2]	8	-128 to 127
[3,0],[2,1],[1,2],[0,3],[4,0]	7	-64 to 63
[3,1],[2,2],[1,3],[0,4],[5,0]	6	-32 to 31
[0,5],[1,4]	5	-16 to 15

Table 1: Model-1: DC and AC coefficients at lowest frequencies.

Coefficient	Size (bits)	Range
[7,7],[7,6],[6,7]	5	-16 to 15
[7,5],[6,6],[5,7]	6	-32 to 31
[7,4],[6,5],[5,6],[4,7]	7	-64 to 63
[7,3],[6,4],[5,5],[4,6],[3,7]	8	-128 to 127
[7,2],[6,3],[5,4]	9	-256 to 255

Table 2: Model-2: AC coefficients at highest frequencies.

Additionally in the following subsections, we show the consequence in the JPEG images, if we apply the cipher algorithm only over the DC coefficients, Section 3.1. In Section 3.2, we show the effect if we apply in the DC and some AC coefficients of the lowest frequencies and in Section 3.3 if applied in the highest frequencies.

3. EXPERIMENTS AND RESULTS

For all of our experiments, we have used the algorithm JPEG in the baseline sequential mode with a Quality Factor (QF) of 100%. For the cipher, we have used the AES in OFB (Output Feedback Block) mode with block and key of 128-bit lengths. However, it can be used with the other possible combination of key and block sizes. The choice of OFB mode is because in this mode, the identical blocks have different ciphered results and the homogeneous areas of the image will not leave visual patterns.

3.1 Encryption of the DC component

Figure 3: Original medical image

After applying the ciphering process only in the DC coefficient and calculating the difference between the original image (EmphysemeInterstitiel 256×256, Figure 3) and the encrypted one, Figure 4, we have gotten the following results, PSNR equal to 9.02 dB and compression ratio equal to 1.87. Without DC encryption the compression ratio is equal to 2.1. We have lost 5.71% because of the encryption process.

We have replaced the encrypted DC values by a static value like 0, 1024 or -1024. For example, if we set the DC=0 for every block, we get the image illustrated in Figure 5. Its PSNR related to the original image is 16.12 dB. We can

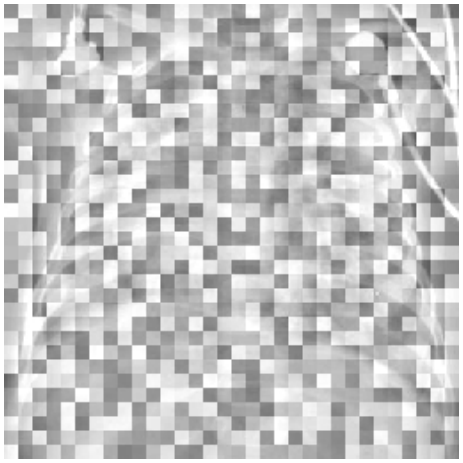

Figure 4: Encryption of the DC component

conclude that, if only the DC component has been encrypted, it is very easy to access the visual information of the JPEG image by simply replacing the ciphered DC coefficient with some constant values. This is because the DC coefficient is highly previsible.

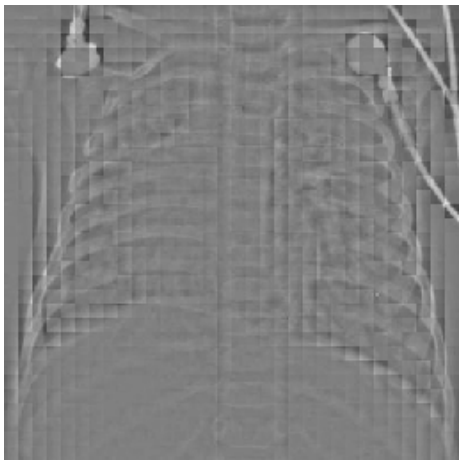

Figure 5: DC=0 in the encrypted image Figure 4

After decrypting with the good key, we get the same image of JPEG (PSNR infinity), that means no loss.

3.2 Selective encryption of the $F(u,v)$ components: low frequencies

In the Section 3.1 we have ciphered only the DC elements. In this section, we show that if we encrypt more elements at the low frequency of each block we get good results. The first model we have created (Table 1) we will take 18 coefficients in the standard zigzag scan of JPEG such that $F(u,v)$ and $u+v \leq 5$. We have defined a predetermined amount of bits for each element according its place in the DCT table. It means that as much as close to the DC element as bigger as its quantity of bits. The total sum of this predefined sizes must be 128 bits, the size of the AES block. The Figure 6 illustrates the result of this method.

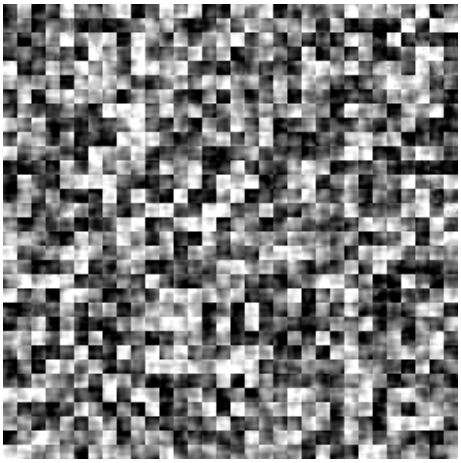

Figure 6: Encryption of the low frequency components

If we calculate the PSNR between the original image and the encrypted one, Figure 6 we will get 9.44 dB. We can notice that the information of the original image is not visible. The compression ratio is equal to 1.51. Then we lose 33.85 % of the encryption because we do not take care of the size of the original coefficients in the decrypted blocks.

We have made some tests to try to guess the DC in a ciphered image. For example, if we substitute the encrypted DC values by a constant value like 0, 1024 or -1024, as it was made in the Section 3.1, it is not possible any more to reconstruct or to have any substantial information about the original image. If we replace the DC of each ciphered block for 0, we get the image illustrated in Figure 7, its PSNR is 13.70 dB.

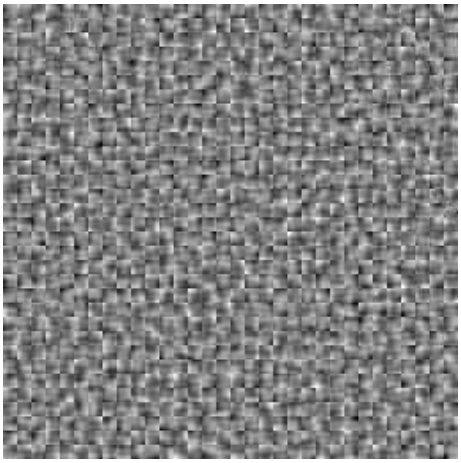

Figure 7: DC=0 in the encrypted image Figure 6

From the table 1, it is noticed that the quantity of bits per coefficient was delimited, therefore we will have truncated values. After decrypting with the good key we lose some information concerning the original image, but these loss are not important as we can see in the decrypted image illustrated in Figure 8. It has a PSNR equal to 41.76 dB.

From the exposed results, we can conclude that is possible to safe an image by SE gaining time and keeping a rea-

Figure 8: Decrypted image Figure 6

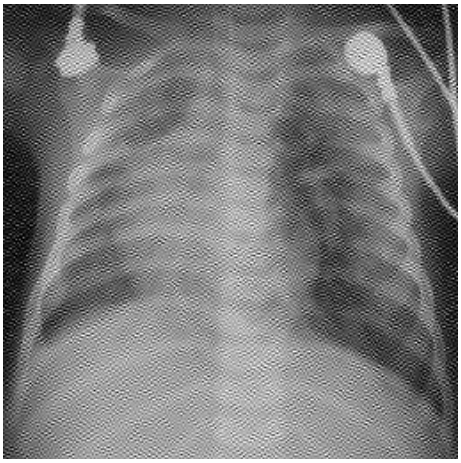

Figure 9: Encryption of the high frequency components

sonable compression rate.

3.3 Selective encryption of the $F(u,v)$ components: high frequencies

All the detailed information of an image is hold by the high frequencies, so if we encrypt only coefficients in this region a big portion of the image can be seen. There are several domains that this kind of encryption is required, such as database searching applications where portions of image data must be visible to allow searching [7]. Applications in education field where images need be partially identified without disclosing the total information. Personal photographs taken from cellular phones.

In this section, we depict some results for the domain where the images must be seen partially, so we apply our method in the high frequencies . We have gotten the results if we encrypt only the highest frequency DCT coefficients. The objective is to allow access an image in modest quality, so if we want to obtain the full quality image we need do decrypt the image with the secret key.

We have encrypted 18 coefficients at the highest frequencies of each block such that $F(u,v)$ and $u+v \geq 9$. They were taken following the standard zigzag path of JPEG. The Figure 9 illustrates the obtained result.

If we calculate the difference between the original image and the encrypted one, Figure 6 the $PSNR = 16.31\ dB$. Then the original image is still visible but we have no details. The compression ratio is equal to 1.23.

In the Table 2, We can notice also that we have truncated values. So, after decrypting with the good key because of the size of some coefficients we lose original information but the decrypted image is very good and the PSNR is equal to 58.98 dB.

4. CONCLUSION

In this paper, we have proposed a new scheme for selective encryption for JPEG images based on AES cipher. We can enumerate some advantages of our method such as combine encryption and compression and allow visualization of the low-resolution compressed image. The experiments show that our method provides satisfactory PSNR, sufficient security and acceptable confidentiality results.

REFERENCES

[1] X. Liu and A. Eskicioglu, Selective Encryption of Multimedia Content in Distribution Networks:Challenges and New Directions. IASTED Communications, Internet & Information Technology (CIIT), November, 2003, USA

[2] W. B. Pennebaker and J. L. Mitchell, JPEG: Still Image Data Compression Standard. *Van Nostrand Reinhold*, 45, 1993.

[3] L. Tang, Methods for Encrypting and Decrypting MPEG Video Data Efficiently. in ACM Multimedia, 1996, pp. 219229.

[4] M. Van Droogenbroeck and R. Benedett, Techniques for a Selective Encryption of Uncompressed and Compressed Images. Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, September 9-11, 2002.

[5] M. Van Droogenbroeck, Partial Encryption of Images for Real-time Applications. Fourth IEEE Benelux Signal Processing, Hilvarenbeek, The Netherlands, 2004, pp.11-15.

[6] M. Fisch, H. Stgner and A. Uhl, Layered Encryption Techniques for DCT-Coded Visual Data. European Signal Processing Conference (EUSIPCO) 2004, Vienna, Austria, September 6-10, 2004

[7] R. Norcen, M. Podesser, A. Pommer, H. P. Schmidt and A. Uhl, Confidential Storage and Transmission of Medical Image Data. Computers in Biology and Medicine 33 (2003), 277-292, Elsevier.

[8] Federal Information Processing Standards Publication 197, "Announcing the Advanced Encryption Standard (AES)" Nov 2001, USA