JPEG2000 2000 Images Protection Sent to Mobile Devices

Ukrania Díaz, Bernardo Alarcos, Enrique de la Hoz, Iván Marsá

[1] Universidad de Alcalá, Departamento de Automática
Escuela Politécnica, Campus Universitario, Alcalá de Henares,
28871 Madrid, España

ukrania@aut.uah.es, bernardo@aut.uah.es, enrique@aut.uah.es, ivmarsa@aut.uah.es

Abstract. With the increasing use of multimedia technologies and mobile devices, also increases the applications which purpose is to offer information or to do advertising by means of the sending of images or videos. In this paper, we approached a digital tourist guide scene in which mobile devices with limited resources need to receive multimedia information across a wireless connection. Also we approached that this information is visible only authorized users. We centre the article on the protection of images on an format of compression adapted. Standard JPEG 2000 has been selected to offer an optimal balance between the quality of image and the occupied space. In order to protect the information, we have worked with selective encryption mechanism, that allow to obtain a relation of commitment between the computational cost, on having concealed the information and the concealment degree.

1. Introduction

This work is located in a scene in which tourist who visit a city use a mobile device that it guide them and allows them to visualize previously images of the places of major interest of the city, beside to offer additional information about this points of interest. For its development we are working with PDA's, who have a GPS to offer information of location and WIFI technology that it allow them to receive information from contents servers, depending of tourist preferences and about their location in a certain zone of the city. The application that the tourist has in the PDA consist of a plane that it locates and is directing him in a certain tourist route, this information is received in a WEB browser. This information can be composed by text, audio, images and video. In the model of business of this application, there offers the possibility that the tourism office that offers this service could rent the PDA's to the tourists and besides it could charge for the service of tourist guide. In this case it is necessary to enable a mechanism of authorization so that only the tourists who have paid to see the information could receive it.

In this article we centre in concretely on the protection of the photographic images of the visited city, having in consideration the limitations of resources of PDA's. We have selected the JPEG2000 format to visualize images, due to its good relation be-

tween compression and quality in photographic images, which it makes appropriate for mobile device. We have centre the study on the selective encryption applied to this case, considering aspects of saving resources.

The rest of the article is constructed of the following form. In section 2 we analyzed briefly the compression scheme and the files format JPEG2000 and the way of applying the selective encryption. In section 3 we proposed a procedure management of keys adapted to the approach scene. Finally, the section 4 is dedicated to conclusions.

2. Selective Encryption Applied to JPEG2000 Images

JPEG2000 is a standard of images compression developed under the auspices of the ISO/IEC JTC1/SC29/WG1 [1], it has been designed to attend the requirements of a diversity of applications like: Internet, colour fax, printing, scanner, digital photography, remote signal, mobile applications and medical images.

It offers several advanced characteristics based on scalability and flexibility, inside these we have[2]: high performance in the compression, multiple resolutions representation, progressive transmission by pixels and resolution precision, lossless and lossy compression, random access and processing image information, bit error resistance, sequential increase capacity and flexible files format.

The technology used by the standard for the compression is the wavelet transformed discreet (DWT), followed of the quantification and ended with the codification. The DWT consists of the decomposition of the image to separate the details in sub-bands. This decomposition can be done by levels, in the first level we obtain four sub-bands: horizontal (LH), vertical (HL), diagonal (HH) and the LL sub-band that is a representation of original image with low resolution. These sub-bands can be decomposed in turn as increases the level of decomposition that normally is realized until obtained a size of 8x8 pixels. Figure 1 shows decomposition scheme at level 3.

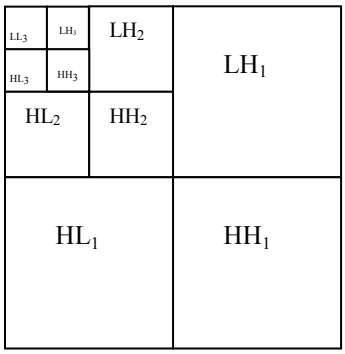

Fig. 1. Descomposición por DWT

A file that contains a compressed image is shaped by a set of boxes an super-boxes, which appear consecutively in the file, we will focus on the box structure called code-stream, where is found it the information of the files, and it is formed by a main header followed by a sequence of tile-streams, these are subdivided in a header of the tile and a pack-stream. A pack-stream can be form by a sequence of packages, each one of this contains a header and the body package [1].

To encrypt an image we have selected a method of selective encryption. The principle of selective encryption implies that only a part of the information content, in this case a image, is encrypted[3], so that the whole image is hide for the one who couldn't decipher the above mentioned portion. Initially it was proposed for video encryption in real time, then it has been proposed in a number of specific applications, specially where it could: to reduce the computational complexity, to add multiple and different encryption systems to the same ciphered file, to permit different ways of organizing the information, or to offer a low quality version that can be viewed by everybody, while the maximum quality version is reserved for those who have contracted the service [4].

Exists different ways of applying the selective encryption on the DWT structure, depending on the part that we decide to encrypt, some authors [5,6] consider encrypting to level of packages, in other cases [7] a part of the bit-stream is encrypted, or to encrypt the sub-bands structure contained in the headers[3].

Our proposal is to encrypt an sufficient percentage of information that allows to hide the image with a cost computational limited. For it we identify the different parts that compose the code-stream, and we focus in the SOD (Start of Data) that is the part where the information begins, from this point we selected the first 10% of the information. We take only a 10% because we consider that encrypting this portion obtain sufficient image distortion and we had select information of the beginning because it is where is contain the most part of the entropy of the image. We can see the result obtain in figure 2.

(a) Imagen original (b) Imagen cifrada

Fig. 2. Imagen Cifrada al 10%

3. Model of Management Keys

In order to carry out the encryption is necessary that, the contents servers and the PDA's share a symmetrical key. We propose that the images should be encrypted online by the user's key requests. Every user will have a different symmetrical key (Ku) which will obtain from a keys server with the previous authorization and payment of the service. This key will give permission for to use the service of tourist guide, defined by means of a few parameters (PS): identifying of user, identifying of PDA's and period of validity of the contracted service.

The contents server will generate the keys (Ku) of dynamical form whenever that an information request comes to its [8], in this way we prevent that it has to store a Ku for every user who accedes to the information. To generate the Ku we will do that these will are depending on the service parameters (PS) and a master key (Km). The master key is share by the contents server and key server. The service parameters will go in the information request in order that the contents server could generate the user's key and encrypt the images (see figure 3).

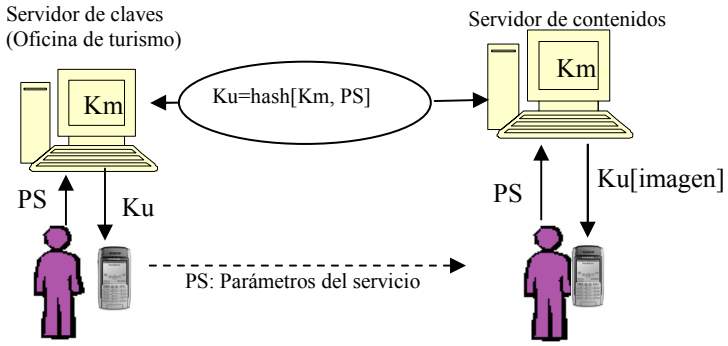

Fig. 3. Gestión de claves

The user's keys are introduced in the PDA's by a secure channel, for example by an infrared port [9] or by channel https if the tourist contracts the service through the net. The master keys will be refreshed every certain period of time to reduce the risk of attacks. If the users don't provide the correct parameters that define the service it will not be able to obtain the information. If a user passes to another user his key and his parameters of service, both users might receive the same service if they are able of supplanting the PDA's identity. To detect this type of attack we can use technologies of intrusion detection based on anomalies of the behaviour. Nevertheless, in view of the low value of the service, it is not probable that this kind of attacks occurs.

4. Conclusion

The encrypting image that we had proposed adapts to the scene in which we want to apply it. On having used devices with low resources, we have a photographic image in format JPEG2000, the one that supports quality in a limited space and with the selective encryption we obtain minimize the computational cost and offer a safety level adjusted to the information's value to protecting.

References

[1] David Taubman, Michael Marcellin : *JPEG2000 Image Compression Fundamentals, Standards and Practice*. Kluwer Academic Publishers (2002).

[2] Daniel T. Lee : *JPEG2000 Retrospective and New Developments.* Proceedings of the IEEE, Vol.93, No.1 (2005).

[3] Yulen Sadourny, Vania Conan : *A Proposal for Supporting Selective Encryption in JPSEC*. IEEE Transactions on Consumer Electronics, Vol. 49, No. 4 (2003)

[4] Tom Lookabaugh : *Selective Encryption, Information Theory and Compression*, University of Colorado, IEEE (2004).

[5] Roland Norcen, Andreas Uhl : *Selective Encryption of the JPEG2000 Bitstream.* IFIP International Federation for Information Processing, LNCS 2828, (2003).

[6] Hongjun Wu, Di Ma : *Securing JPEG2000 Code-Streams.* IEEE (2004)

[7] Andreas Pommer, Andreas Uhl : *Selective Encryption of Wavelet Packet Subband Structures for Obscured Transmission of Visual Data*. 3er edición, IEEE Benelux Signal Processing Symposium, Leuven, Belgium (2002)

[8] Stajano F, Anderson R. : *The resurrecting duckling: Security issues for ad-hoc wireless networks*. Security Protocols, 7th International Workshop Proceedings (1999).

[9] Bernardo Alarcos, Marifeli Sedano, and Maria Calderón. : *Multidomain Network Based on Programmable Networks: Security Architecture*, ETRI Journal, vol.27, no.6, ISSN 1225-6463 (2005) 651-665.