Scalable Access Control for JPEG 2000 Encoded Images Using JPSEC Protection Tools

Ayman Haggag, Mohamed Ghoneim, Jianming Lu, and Takashi Yahagi
Graduate School of Science and Technology,
Chiba University
Chiba Shi, 263-8522 Japan
Email: aymanh@graduate.chiba-u.jp

Abstract—In this paper we first give a brief discussion of the newly emerging JPSEC security standard for JPEG 2000 compressed image. We then propose a scalable access control scheme specially designed for JPEG 2000 encoded images. Our scheme applies SNOW 2 stream cipher to JPEG 2000 codestreams in a way that it is possible to truncate the JPEG 2000 codestream after encryption, during transmission, storage, or by a third party unaware of the encryption key, and still be possible to decrypt the image to view it at a lower resolution or a quality level. We propose three implementations for our algorithm. Packet Based Access Control in which individual packet bodies are encrypted using the same encryption key and provides near optimum Rate Distortion truncation. Resolution Based Access Control and Quality Based Access Control in which each entire resolution or quality layer is encrypted using a different encryption key and provide controlled access to various resolutions or quality layers depending on the level of the key given to the user. Encryption keys are dependent of each other such that the key for a lower resolution or quality layer is the result of hashing the key of the higher resolution or quality layer. The hashing function used is the SHA-256. Our access control scheme preserves the inherent flexibility and accessibility of JPEG 2000 encoded images, and also preserves end-to-end security of encrypted images.

I. INTRODUCTION

JPEG 2000 is a new image coding standard established by the Joint Photographic Experts Group (JPEG) and became an International Standard in August 2000. This new image coding standard referred to as Part 1 of the JPEG 2000 specifications [1] supports many new features. Among the new features provided by JPEG 2000 is the process of transcoding. Transcoding is a process that modifies a JPEG 2000 codestream without decoding and re-encoding the image. In this process, a JPEG 2000 encoded image can be directly transcoded to an image of lower resolution, quality layer, color component or spatial region without the need to decode and re-encode the whole JPEG 2000 image. Also a received JPEG 2000 image can be transcoded by simply discarding higher order resolutions or quality layers and constructing the image at a lower resolution or at a lower quality. For example, reducing the resolution simply requires extracting a subset of resolution levels. Likewise, reducing the bit rate simply requires extracting a subset of quality layers, the transcoding process is shown in Fig. 1. A detailed study of JPEG 2000 standards is presented in [2].

Image security is becoming an important demand, meanwhile the inherent flexibility of JPEG 2000 has to be preserved. It is highly desirable after generating and securing a JPEG 2000 codestream to allow untrusted transcoders at intermediate network nodes to perform downstreaming of the JPEG 2000 codestream discarding resolutions, quality layers or spatial regions, to match the diverse receivers’ capabilities, as shown in Fig. 2. This must be done without decrypting the image at intermediate network transcoders and without access to security keys and thus preserving end to end security. It is also important to be able to control the level of access granted to an image viewer, for example, two users receiving the same JPEG 2000 encoded codestream, one user should be able to decrypt and view the full resolution or quality of the image.
and the other should be able only to decrypt and view a lower resolution or quality, depending on the decryption key given.

In the mean time, a new security standard is being developed and integrated in the JPEG 2000 coding standards, it is referred to as JPEG-2000 Part 8 or JPEG 2000 Secured (JPSEC) that is meant to provide security services for JPEG 2000 images. The JPSEC currently reached the FDIS (Final Draft International Standard) stage [3]. While it is being developed, it is very important to adapt this future security standard in newly developed security services for JPEG 2000 images.

Image access control has been previously targeted in a variety of ways. File level encryption is a method where the whole image file is encrypted. This method is very simple but it prohibits all JPEG 2000 features such as scalability and access to various image resolutions, qualities, or spatial regions. Another method proposed in [4] is called Pseudo-random inversion of coefficients signs. This method allows a preview of low resolution(s) of an image, whilst preventing the correct display of its higher resolutions by introducing a pseudo-random noise in the high frequencies subbands.

In this paper we first give a brief overview of the new JPSEC standard in section II. In section III we present our new proposed Access Control method and propose 3 different implementations for this method. In section IV we provide evaluation and results, and section V is a conclusion and summary.

II. JPSEC OVERVIEW

JPSEC is a very flexible and open framework, it provides a wide range of predefined security service tools in what is called JPSEC normative tools that uses predefined Template protection tools to implement image resolutions, qualities, or spatial regions. The same time, JPSEC also provides an extensible open framework for JPSEC non-normative tools that contain future tools that can be privately developed and defined by the user or registered through a Registration Authority (RA).

Template protection tools contain different protection templates to target a wide range of protection services. Three protection templates are defined in JPSEC [3]: Decryption template, Authentication template, and Hash template.

Decryption template supports three cipher modes: Block cipher mode using AES, TDEA, MISTY1, Camellia, Cast-128 or SEED cipher types, Stream cipher mode using SNOW 2 cipher type, and Asymmetric cipher mode using RSA cipher type.

Authentication template contains three general classes of authentication methods: Hash-based authentication also referred to as (Hash-based MAC), Cipher-based authentication referred to as (Cipher-based MAC), and Digital Signature methods. Hash-based Authentication template supports ten hash functions: SHA-1, RIPEMD-128, RIPEMD-160, MASH-1, MASH-2, SHA-224, SHA-256, SHA-384, SHA-512, and WHIRLPOOL. Cipher-based Authentication template only supports CBC-MAC authentication method. Digital Signature template supports four digital signature methods: RSA, Rabin, DSA, ECDSA methods.

Hash template is a key-less integrity check that utilizes the same ten hash functions used by the Hash-bashed Authentication template mentioned before.

Key Information template is used to communicate key information using X.509 Certificate with encoding role: DER or BER, or URI for certificate or secret key.

JPSEC introduced two new marker segments in the JPEG 2000 codestream to signal security syntax. The SEC marker presented in the Main Header, and an optional INSEC marker that can be inserted anywhere in the bitstream to provide additional or alternative security signaling.

The SEC marker segment supports specifying multiple security tools as well as the Zone of Influence ZOI which describes the data associated with each protection tool. The ZOI may contain one or more zones, and in this case the influenced zone is their union. The ZOI may use Image related description classes that specify the region in terms of Image region, Tile, Resolution, Layer, Component, Precinct, Packet, Sub-band, or Code-block. On the other hand, it may also use non-image related description classes that specify the region in terms of: Byte range starting after the SOD or the SEC markers, Padded byte range, Packet range, Distortion, or TRLCP tags.

The Processing Domain (PD) is used to indicate at which domain the protection method is used. There are four possible domains: Pixel domain, Wavelet coefficient domain, Quantized wavelet coefficient domain, and Codestream domain.

Granularity Level (GL) is also used to indicate the unit of protection for each protection method. The granularity syntax may define if the unit of protection is a tile, tile-part, component, resolution level, layer, precinct, packet, sub-band, code-block, or a zone identified in ZOI and for each unit whether the header part is protected or not protected.

The Processing Order (PO) defines the processing order used when applying the protection tool to the codestream, there are five processing orders supported: Tile Resolution Layer Component Precinct, Tile Component Precinct Resolution Layer, Tile Layer Resolution Component Precinct, Tile Precinct Component Resolution Layer, and Tile Resolution Precinct Component Layer.

The INSEC marker segment present in the bitstream itself can be used to give additional or alternative parameter for one of the security tools. The INSEC marker must reference one tool by using its instance index specified in the SEC marker.

III. PROPOSED ACCESS CONTROL METHODS

Our proposed methods are applied directly to JPEG 2000 codestream bearing in mind any possible operation such as transcoding (parsing or scaling), especially accessing a JPEG 2000 encoded image at a lower resolution or at a lower quality level, so the Processing Domain (PD) is set to Codestream domain. In all our proposed design approaches we will use the Stream cipher template of the Decryption template specified in the JPSEC standard. The applied access control method will be signaled in the SEC marker in the main header marker segment using standard JPSEC signaling.
Our proposed method works as follows: During the JPEG 2000 encoding process, the image undergoes four operations: Wavelet transform, embedded scalar quantization, entropy coding and codestream building as shown in Fig. 3. A JPEG 2000 codestream consists of a header followed by packets of data. In each packet appears the codewords of the codeblocks that belong to the same image component, image resolution and layer. Thus a packet corresponds to a body, with the coding-passes codewords, and a header that contains identification and information about the corresponding codeblocks. There are 5 progressing modes supported by JPEG 2000: LRCP, RLCP, PCRL, and CPRL, where L is Layer, R is Resolution, C is Component, and P is position.

After an image in encoded according to JPEG 2000 standards and the codestream is generated. Our encryption Granularity Level (encryption unit block) is selected. There are three alternatives for selecting the Granularity Level: individual packet, entire resolution, or entire quality layer. The encryption unit block is then feed to the encryption algorithm.

We selected the SNOW 2 stream cipher as our encryption algorithm. The SNOW 1 stream cipher is a new word-based synchronous stream cipher developed by Thomas Johansson and Patrik Ekdahl at Lund University in 2000 [5] and its modified version SNOW 2 was adapted as an International Standard in 2005 [6]. The design of the cipher is quite simple, it consists of a linear feedback shift register, feeding a finite state machine as shown in Fig. 4. This cipher uses an encryption key of length 128 bits or 256 bits. In our method we will utilize the 256-bit key for higher security.

A. Packet Based Access Control

In this approach, the Granularity Level (GL) is set to a single packet. Each individual JPEG 2000 packet is fed to the encryption algorithm and the encrypted data is stored in place of the packet body. Only the packet body is encrypted and the packet header is left unencrypted. The encryption procedure is shown in Fig. 5.

B. Resolution Based Access Control

This approach considers the special case when the JPEG 2000 image is ordered in RLCP or RPCL progression, which is also called resolution progression. In this special case we assume that scaling will probably be carried out by discarding higher resolution levels. In this case, each resolution level is represented by a contiguous data segment as shown is Fig. 6, and scaling is carried out by discarding whole resolutions. Thus Granularity Level (GL) is set to entire resolution level and Each entire resolution is fed to the encryption algorithm and the encrypted data is stored in place. Data from each individual resolution level is encrypted using a different encryption key, but those keys are independent of each other through a hash function. The 256 bits of the encryption key for the highest resolution level is selected arbitrarily, the encryption key for the next lower resolution level is the result of hashing the encryption key of the higher resolution level as show in Fig. 7. The hashing function used is the SHA-256, this hashing function is FIPS (Federal Information Processing Standards)
approved [7] and the length of its hashing output is 256 bits which matches the encryption key length of 256 bits used with the SNOW 2 algorithm.

C. Quality Based Access Control

In a similar approach when the JPEG 2000 image is ordered in LRCP, which is also called quality layer progression, and it is also assume that scaling will probably be carried out by discarding higher order quality layers, each quality layer will be represented by a contiguous data segment and scaling is carried out by discarding whole quality layers. Similarly, Granularity Level (GL) is set to entire quality layer. Each entire quality layer is fed to the encryption algorithm and the encrypted data is stored in place. Each quality layer is encrypted using a different encryption key, and encryption keys for each individual quality layer are generated in a way similar to the previous method.

IV. EVALUATION AND RESULTS

A full feature JPEG 2000 codec is implemented in JAVA [8]. The JPSEC syntax is implemented to signal decryption parameters as described above. Our proposed methods are tested on several JPEG 2000 encoded images with different encoding parameters and progressions.

In this section, first we will compare our packet based authentication to the Pseudo-random inversion of coefficients signs proposed in [4] and then we will compare resolution based and quality layer based authentication to packet based authentication and then the overall proposed methods are evaluated and the results of comparison are summarized.

A. Packet Based Access Control

This method provides the maximum flexibility in transcoding JPEG 2000 encoded image as the packet is the smallest building unit in a JPEG 2000 codestream. A mid network transcoder has total freedom in parsing the JPEG 2000 codestream. This preserves the end to end image security. If the image is to be scaled and viewed at a lower resolution, a lower quality or a lower spatial region, corresponding packets are discarded and the image can still be decrypted. It is also possible using this method to truncate packet parts for fine granularity near optimum Rate Distortion scalability.

The disadvantage of this method is that it is not possible to grant different levels of access to user by using different keys, as this method uses a single key to encrypt and decrypt the whole JPEG 2000 codestream. This method also results in the highest computation complexity, to reinitialize the SNOW 2 cipher encoder for each individual packet.

Comparing this method to the method proposed in [4], we find that our method results in a much faster processing for encryption and decryption of JPEG 2000 images. This increase in the speed of our method is due to the fact that our method is performed on the final codestream rather than between the entropy coding and the rate allocation procedures of the JPEG 2000 code stream as in [4], so encryption and decryption can be done on the fly without the need to decode and re-encode the JPEG 2000 image.

B. Resolution Based Access Control

This method, compared to the Packet Based Access Control method, greatly reduces the processing complexity and increases the processing speed by reducing the number of times the SNOW 2 cipher algorithm needs to be reinitialized to encrypt and decrypt the JPEG 2000 codestream. This is because the SNOW 2 cipher algorithm needs to be reinitialized only for each resolution level, not for each packet as in the Packet Based Access Control method.

This method has another advantage that, it is possible to grant access to various resolution levels by sending the appropriate decryption key to the image recipient. Fig. 8 shows the image Bath accessed at two different resolutions. On the other hand, using this method it is not possible to parse the JPEG 2000 image to change its progression order or to truncate packets or packet parts for fine granularity scalability like the Packet Based Access Control method, and scalability is only limited to resolution scalability.
C. Quality Based Access Control

This method, similar to the Resolution Based Access Control method, reduces complexity and increases the processing speed by limiting the number of time the SNOW 2 cipher algorithm needs to be reinitialized to the number of quality layers in the JPEG 2000 image, but this method also prohibits parsing and fine granularity scalability compared to the Packet Based Access Control method, and scalability is only limited to quality scalability.

Also this method has the advantage that, it is possible to grant access to various quality layers by sending the appropriate decryption key to the image recipient.

Table 1 summarizes the comparison between our three proposed methods in terms of features and processing complexity.

<table>
<thead>
<tr>
<th>Access Control Method</th>
<th>Processing Complexity</th>
<th>Parsing Scallability</th>
<th>Scallability of Access Control of Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Based</td>
<td>High</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Resolution Based</td>
<td>Low</td>
<td>Not available</td>
<td>Resolution By Resolution</td>
</tr>
<tr>
<td>Quality Based</td>
<td>Low</td>
<td>Not available</td>
<td>Quality By Quality</td>
</tr>
</tbody>
</table>

V. Conclusion and Summary

In this paper first we gave an introduction to some of the new features of JPEG 2000 coded images and the need to provide security services that do not prohibit those features. We then followed by a brief discussion of the newly emerging security standard JPSEC that is specially designed for JPEG 2000 coded images and will be integrated in the JPEG 2000 standards. Then we discussed the previous solutions for image Access Control and presented our new Access Control method with three different implementation approaches and compared between them. Evaluation and results showed the efficiency and the flexibility level of the three proposed design alternatives and the trade off between system complexity and overhead processing time on one side and the degree of flexibility, transcodability, scalability of the protected JPEG 2000 images on the other side.

REFERENCES