PROGRESSIVELY AUTHENTICATED IMAGE TRANSMISSION*

Małgorzata Steinder
Sami Iren
Paul D. Amer

Computer and Information Science Department
University of Delaware, Newark, DE 19716 USA
Email: {steinder,iren,amer}@cis.udel.edu

Abstract

Network-conscious image compression has been shown to provide faster progressive display than traditional compression algorithms, when images are transmitted over lossy low-bandwidth packet-switched networks. In this paper, we combine the advantages of wavelet-based, network-conscious image compression with a blind digital image signature technique. Together these two approaches investigate progressive display where each progressive image can be authenticated by the receiver in real time.

1 INTRODUCTION

Image transmission over wireless networks requires special attention mainly for two reasons. (1) Wireless networks typically provide low bandwidth and unreliable communication. Image data, on the other hand, by its nature, requires high bandwidth. Therefore, transmitting images over these low bandwidth networks takes much more time than it would over a typical Internet connection. Many image transmission applications, such as telemedicine and intelligence gathering, are time-critical where being able to display the most important information in the shortest period of time is crucial. Our work on network-conscious image compression emphasizes this fact and motivates a new design approach to compression algorithms [6]. One particular implementation of network-conscious GIF image compression illustrates the advantage of using this approach when transmitting over lossy packet-switched networks [1].

(2) For insecure environments it is possible for an enemy to tamper with images during transmission. Thus authenticating images at the receiver before making a decision based on them is important. Digital signatures are often used for this authentication. They can be implemented by watermarking a transparent signal into an image. The digital signature should be "blind". That is, the receiver should not need to know the original image and the original watermark in order to verify an image's authenticity [15].

One drawback of current watermarking schemes is that they require the complete image data before authentication can be performed. Even though an image can be progressively displayed at the receiver, the digital signature cannot be verified until the complete image is received. This requirement, however, reduces the usefulness of progressive display. In this research, we investigate a method which combines advantages of wavelet-based network-conscious image compression with a blind digital image signature technique. Together the two approaches can progressively authenticate pieces of image data as they arrive.

Section 2 discusses advantages of network-conscious compression for progressive display of images. Section 3 explains how authenticity of images can be verified based on partial data by using a wavelet-based approach.

2 NETWORK-CONSCIOUS IMAGE COMPRESSION

A network-conscious compressed image is one that is encoded *not* simply to give the *smallest size* for a specified image quality, but to give the *best (i.e., smallest) response time - image quality* combination to an end user retrieving the image over a packet-switched network [5, 8]. The basic characteristics of a network-conscious compressed image are: (1) application level framing [2], (2) progressive display (preferably multi-layered), and (3) robustness and adaptiveness to different user needs and various networking conditions.

The key feature of network-conscious image compression is that it produces path-MTU-size[1] self-contained blocks (ADUs) that can be decompressed independently of each other. When these blocks are transmitted over a lossy network, they can be received and processed out-of-order, thereby permitting better progressive display. ADUs permit the use of a more efficient transport pro-

* Prepared through collaborative participation in the Advanced Telecommunications/Information Distribution Research Program (ATIRP) Consortium sponsored by the U.S. Army Research Laboratory under the Federated Laboratory Program, Cooperative Agreement DAAL01-96-2-0002. This work also was supported, in part, by the US Army Research Office (DAAH04-94-G-0093).

[1] MTU is the maximum frame size that a link layer can carry. A path MTU-size ADU is one that can be transmitted end-to-end without the need for IP layer fragmentation and reassembly.

tocol that does not need to preserve order. This is particularly important in a wireless environment [8].

Assuming some loss, the expected amount of buffer space required at the transport receiver for an unordered protocol is always less than the space required for ordered protocols [12]. Furthermore, out-of-order delivery of ADUs reduces the jitter at the receiving application. In ordered transport protocols, ADUs that are received out-of-order are kept in the buffers. When missing ADUs finally arrive, ADUs waiting in the buffer are delivered as a group to the application. This approach makes the delivery of ADUs to the application more bursty. The burstiness may result in bottlenecks at the receiving application [3].

Another advantage of compressing an image into ADUs is that the transmission of each ADU can be tailored to its particular characteristic. Not all parts of image data are uniform and require the same QoS. For example, low frequency coefficients (i.e., important data) of a wavelet image require a reliable service. On the other hand, high frequency coefficients (i.e., less important details) can tolerate a certain level of loss. Independent ADUs enable the use of different QoS such as reliability and priority for each ADU type.

Network-conscious compressed images are robust and can also adapt to different networking conditions easily. A lost or bit-errored packet will not destroy an entire image. A network-conscious compressed image can be transmitted over a very low bandwidth lossy network as well as a high bandwidth reliable network. The same compressed image can even be used, without any modifications, in a multipoint communication, where each participant has different requirements.

3 AUTHENTICATION OF IMAGES

In a system that progressively displays images in an insecure environment, it is important to verify images as authentic as soon as possible at the receiver. Prompt verification of image authenticity is crucial when a time critical decision has to be made based on the displayed image. In this research, we incorporate a wavelet-based progressive authentication method into our network-conscious SPIHT algorithm [7].

Watermarking is a technique for digitally signing an image. A transparent signal is inserted into an image such that no visible difference exists between the original image and the signed image. We use a blind watermarking technique meaning that the original image need not be known to verify the signature. The embedded signal carries information necessary to verify the integrity of the image, and as a watermark, the information is hidden. Even a careful observer cannot distinguish between a watermarked and unwatermarked image. The watermark information is based on the content of the image, such as its edge map [14, 15].

Our initial approach was based on the fact that the low-low (LL) band contains the most important information of the image [4]. We conjectured that once the LL band data is verified, any modifications introduced by tampering with other bands will be either insignificant (with regard to the contents of the image), or easily noticeable by human eye.

Figure 1 illustrates our watermarking scheme at the sender. First, the original image is transformed into the wavelet domain. Then, the LL band of wavelet coefficients constituting a rough image is scaled to a size determined by the number of watermark bits that fit into the LL band. Next, an edge map of the scaled, rough image is computed and encrypted using the DES algorithm's CBC mode [13].

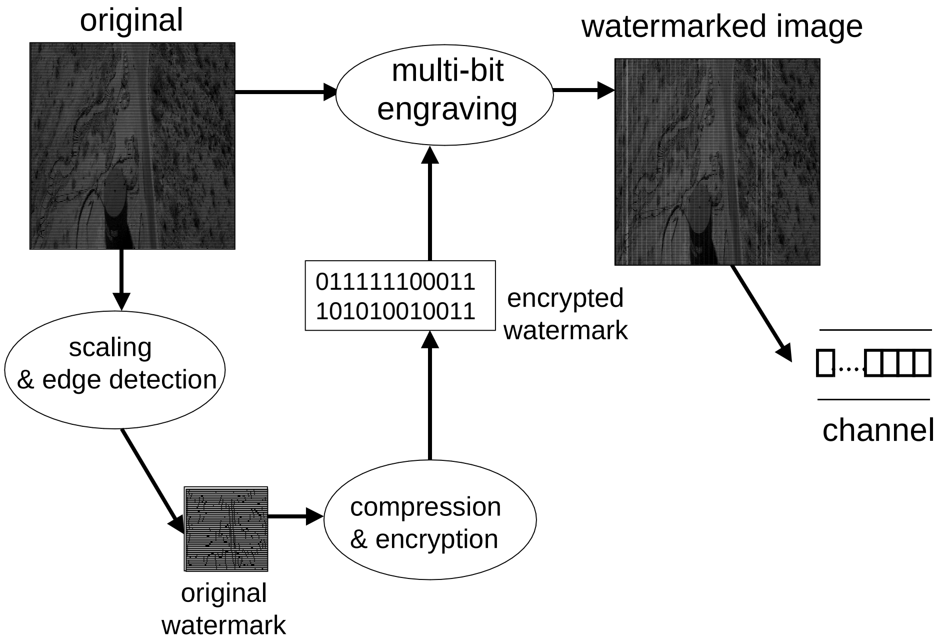
The encrypted sequence of bits constitutes the watermark. This watermark is inserted into the LL band of wavelet coefficients. The watermarked matrix of coefficients is then encoded using network-conscious SPIHT algorithm and transmitted. This algorithm divides the coefficients into ADUs. ADUs containing the LL band coefficients are transmitted first by using an unordered no-loss transport service [9]. Other ADUs are transmitted later by using an unordered no-loss, controlled-loss, or uncontrolled-loss transport service. Choice of transport service largely depends on network conditions and the desired image quality.

An image may be signed using single- or multi-bit engraving. To sign an image with single-bit engraving [15], three coefficients in the LL band are analyzed at a time. They are sorted, and their range is divided into intervals. The size of an interval is $\frac{1}{8}$ of the mean of maximum and minimum of the three values. Subsequently, the median is modified by shifting it to a border of the interval it belongs to. Whether it is shifted towards the larger or smaller value depends on the value of the watermark bit to be engraved. Multi-bit engraving takes advantage of the fact that in many cases the size of the interval is much greater that the encoding threshold[2]. In such a case the interval is divided further into smaller subintervals of size equal to the encoding threshold. The median is shifted to one of the points marked by borders of these subintervals. This point is chosen based on a value formed by a number of consecutive watermarked bits. Since the number of points within an interval is ≥ 2, the number of watermark bits used to choose a point is ≥ 1. Therefore, multi-bit engraving allows to increase watermark bit capacity of a coefficient matrix [15].

This watermarking technique makes it possible for a receiver to verify authenticity of an image as soon as the LL band of its coefficients is received. As presented in Figure 2, the receiver first extracts the watermark from the received parts of the image. It scans the LL band analyzing all coefficient triplets. The watermark bit is determined by examining the median and finding out to which interval it belonged before modification and in which direction it was shifted. Then, the receiver computes its own watermark using the same algorithm as the sender, and compares the result to the extracted watermark. If the signatures are equal the entire image is considered valid.

Note that the sender and receiver do not use the same coefficients to calculate the signature. Since the receiver does not have the

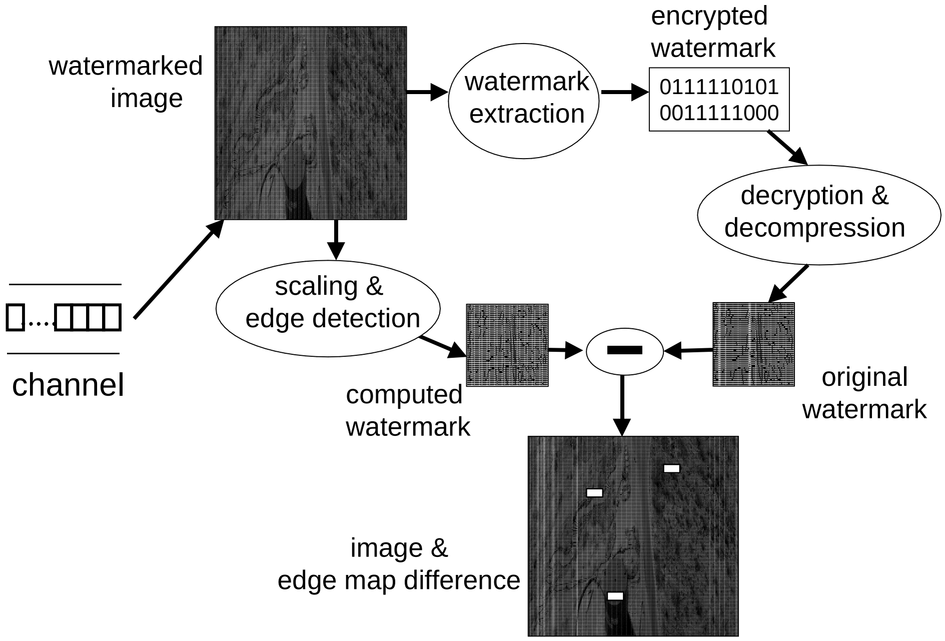
[2] Encoding threshold is the smallest difference between coefficients that makes the coefficients be encoded as different values



32×32, only 320 bits may be engraved into it using single-bit engraving. To compute a watermark for a 512×512-pixel image, it must be resized with a large scaling factor (e.g, 30 in each dimension). Such scaling results in the loss of many details. Therefore, it is possible that watermarks computed for an original and a cleverly tampered image to be the same. With a small LL band, it is also possible to modify other parts of the coefficients matrix in such a way that a tampered image appears authentic. In this case, although the LL band will be verified as valid, the receiving user may be shown a tampered image.

A significant improvement results from increasing the amount of content information conveyed in a watermark. Two possible techniques are: (1) compressing the watermark before inserting it, and (2) multi-bit engraving [11]. We have been using arithmetic coding [10] compression, which resulted in increasing the signature size by a factor of 2. By using multi-bit engraving, the number of watermark bits that fit in the LL band was further increased $1.5-5$ times depending on the number of encoding bits.

Another solution to this limitation is choosing a larger size LL band. It has been empirically estimated that the minimum safe size of the LL band should be at least 1/64 of the original image. However, increasing the size of the LL band tends to reduce the compression performance of the SPIHT algorithm.



[3]The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.

[7] S. Iren, P. Amer, and P. Conrad. NETCICATS: network-conscious image compression and transmission system. *Lecture Notes in Computer Science: Advances in Multimedia Information Systems*, 1508:pp 57–68, September 1998.

[8] S. Iren, P. Amer, and P. Conrad. Network-conscious compressed images over wireless networks. *Lecture Notes in Computer Science: Interactive Distributed Multimedia Systems and Telecommunication Services*, 1483:pp 149–158, September 1998.

[9] S. Iren, P. Amer, and P. Conrad. The transport layer: Tutorial and survey. *ACM Computing Surveys*, June 1999.

[10] G. G. Langdon Jr. An introduction to arithmetic coding. *IBM Journal of Research and Development*, 28:135–149, March 1984.

[11] G. Arce L. Xie. A joint wavelet compression and authentication watermarking. In *IEEE International Conference on Image Processing*, Chicago, IL, Oct 1998.

[12] R. Marasli, P. Amer, and P. Conrad. An analytic model of partially ordered transport service. *Computer Networks and ISDN Systems*, 29(6):675–699, May 1997.

[13] B. Schneider. *Applied Cryptography: protocols, algorithms, and source code*. Wiley, New York, 1996.

[14] X. Xia, C. Boncelet, and G. Arce. A wavelet watermark for digital images. In *Advanced Telecommunications/Information Distribution Research Program*, College Park, MD, February 1998.

[15] L. Xie and G. Arce. A blind content based digital image signature. In *Advanced Telecommunications/Information Distribution Research Program*, College Park, MD, February 1998.