Re-quantization Based Semi-Fragile Authentication for General Uniform Quantizer

Bo Shen, Ton Kalker
Hewlett-Packard Laboratory
1501 Page Mill Road MS 1181, Palo Alto, CA 94304
Email: {bo.shen, ton.kalker}@hp.com

***Abstract*— Semi-fragile authentication schemes are found to be useful to maintain authentication in the event of certain allowed manipulation of source content. This paper focuses on a quantization based algorithm, and extends it to more general uniform quantizers. Earlier work is found to be a special case of our generalized solution which provides more useful guideline when selecting quantizer for this type of authentication. Experimental results verified our analytical conclusion.**

***Index Terms*— Authentication, Uniform scalar quantizer, Re-quantization**

I. Introduction

Many semi-fragile authentication schemes [1] have been proposed to be resistant to certain manipulation of source content. One type of these schemes is resistant to transcoding based on re-quantization [2][3].

Figure 1 shows the set-up of an authentication system that is resistant to quantization-based compression. At the signing stage, (a subset of) the raw source coefficients are quantized by a coarse quantizer $\mathbf{Q}_a$ (with quantization step size s_a). The resulting values $\mathbf{Q}_a(x)$ are converted into a digest $d = \mathbf{H}(\mathbf{Q}_a(x))$, where $\mathbf{H}$ is an appropriate hash function. This value d is subsequently signed (not shown in the figure) using a private key K_r and the signature $E_{K_r}[d]$ is transmitted to the receiver. The values $y = \mathbf{Q}_a(x)$ constitute the stream of signed coefficients. This signal y may be subjected to further quantization with a quantizer $\mathbf{Q}_e$, resulting in coefficients $z = \mathbf{Q}_e(y)$. The receiver verifies the authenticity of a received signal z by repeating the procedure at the encoder and comparing its computed hash value with the signature d provided by the signer.

The key for this type of authentication scheme to be valid is the following exact reconstruction property first found in [2].

Definition 1 (Exact Reconstruction): A pair of quantizers $(\mathbf{Q}_1, \mathbf{Q}_2)$ is said to have the exact reconstruction (ER) property if and only if for all x and $z = \mathbf{Q}_2(x)$

$$\mathbf{Q}_2\mathbf{Q}_1(z) = z. \tag{1}$$

One easily verifies that if the pair $(\mathbf{Q}_e, \mathbf{Q}_a)$ has the exact reconstruction property, then the authentication scheme sketched above will work.

Note that the subset of coefficients used for authentication is quantized by $\mathbf{Q}_a$ before the encoding stage. The quality degradation is always there since s_a is in practice always larger than s_e. This might raise the obvious question why any second coding phase with quantizer $\mathbf{Q}_e$ is needed. However, in JPEG or video compression practice, the quantizer step size is selected at the level of macro-blocks (minimally) and applies to a group of coefficients. This group of coefficient includes both coefficients that are used for authentication and those that are not. The rate-distortion tradeoff still needs to be managed by the step size selection for the coefficients that are not used for the authentication.

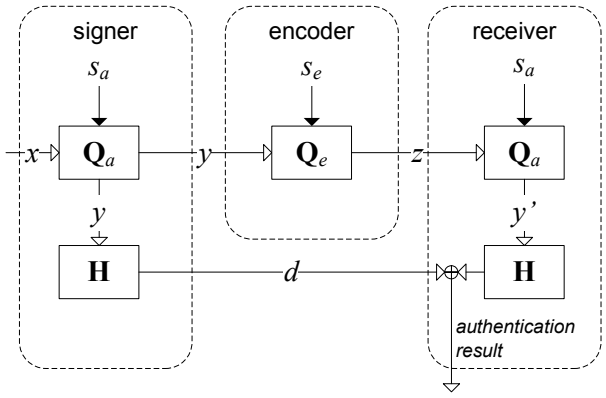


Fig. 1. Authentication system for quantization-based compression.

Previous work [2][3] has reported on this method in the context of compression systems that rely on a specific scalar quantizer with the reconstruction level at the absolute centroid of quantizer bins. In video compression, especially for inter frames, the location of reconstruction level within quantizer bin may vary due to rate-distortion considerations. In this paper, we investigate this exact reconstruction property for general uniform scalar quantizer. This analysis provides better guideline on how to select $\mathbf{Q}_a$ that preserves the exact-reconstruction property in the context of various compression scenarios (with different $\mathbf{Q}_e$).

In the next section, we start with defining the generalized uniform quantizer and follow with derivation of the general condition for exact reconstruction. In Section II-D, we provide discussions in the context of different compression standards. Experimental results are presented in Section III. We conclude this paper with a summary of the results in Section IV.

II. Generalized Analysis on Exact Reconstruction

In this section we prove our main result on conditions for exact reconstruction. We start by providing a model for

quantization.

A. Dead-Zone Quantizers

A general dead-zone scalar quantizer Q is often modeled as follows. Given input x, quantization output q is produced as

$$q = Q(x) = \begin{cases} sign(x) \left\lfloor \frac{|x|}{s} + \varepsilon \right\rfloor, & \frac{|x|}{s} + \varepsilon > 0 \\ 0, & otherwise \end{cases}, \quad (2)$$

where s is the quantizer step size, and ε controls the size of the deadzone. Typically, $\varepsilon \in [0, 1)$, and it also represents how the division is rounded. For example, $\varepsilon = 0$ or 0.5 are often used for deadzone sizes of $2s$ or s, respectively. The quantizer interval for quantizer bin q can be obtained as:

$$Interval = \begin{cases} [-(1-\varepsilon)s, (1-\varepsilon)s), & q = 0 \\ [(q-\varepsilon)s, (q+1-\varepsilon)s), & q > 0 \\ [(q-1+\varepsilon)s, (q+\varepsilon)s), & q < 0 \end{cases}. \quad (3)$$

Reconstruction is obtained by inverse quantization Q^{-1} which is defined as:

$$\hat{x_q} = \begin{cases} 0, & q = 0 \\ (q-\varepsilon+\delta)s, & q > 0 \\ (q+\varepsilon-\delta)s, & q < 0 \end{cases}. \quad (4)$$

Here $\delta \in (0, 1)$ to make sure the reconstruction level resides within its corresponding quantizer bin.

B. Uniform Quantizers

In order to ease our subsequent mathematical analysis, we will slightly modify our definition of a quantizer.

First, the exact reconstruction property as defined in Definition 1 has a slightly different notion of a quantizer than as defined in the previous section. More precisely, in Definition 1 quantizers are assumed to be a combination of a quantizer and an inverse quantizer as above. As this is all we need, we will assume in the remainder of this paper that our quantizers include reconstruction.

Second, dead-zone quantizers are mathematically difficult to analyze in the neighborhood of 0. However, sufficiently far away from 0, dead-zone quantizers behave uniformly (to be defined below). Therefore we will study uniform quantizers first and comment on the impact of the non-uniform behavior around 0 later. We are now able to state our definition of a uniform quantizer.

Definition 2 (Uniform Quantizer): A uniform quantizer $\mathbf{Q}(x) = \mathbf{Q}(s, \varepsilon, \delta)(x)$ with parameters s, ε and δ is defined by

$$\mathbf{Q}(x) = (\left\lfloor \frac{|x|}{s} + \varepsilon \right\rfloor - \varepsilon + \delta)s. \quad (5)$$

Note that a uniform quantizer partitions the set of real numbers $\mathbf{R}$ in intervals $I_q = [B^q, B^{q+1}]$ of size s, where $B^q = (q-\varepsilon)s$. Moreover, elements of I_q are reconstructed at the point $B^q + \delta s$.

C. Condition for Exact Reconstruction

We now derive the general condition as defined in Definition 1. Equation (1) implies that x is a reconstruction level of $\mathbf{Q}_2$. Denoting B_2^j as the left boundary of bin j for $\mathbf{Q}_2$, we have, $x = B_2^j + \delta_2 s_2$. Denoting $y = \mathbf{Q}_1(x)$, we have $y = B_1^i + \delta_1 s_1$. Note that i and j are the quantized coefficient index of x for Q_1 and Q_2, respectively.

Equation (1) also implies that x should be within the interval of bin i for $\mathbf{Q}_1$ and that y should be within the interval of bin j for $\mathbf{Q}_2$. Mathematically, we have

$$\begin{cases} B_1^i \le x < B_1^i + s_1 \\ B_2^j \le y < B_2^j + s_2 \end{cases}. \quad (6)$$

Plugging in x and y with some manipulation, we have

$$\begin{cases} \delta_2 s_2 - s_1 < B_1^i - B_2^j \le \delta_2 s_2 \\ -\delta_1 s_1 \le B_1^i - B_2^j < s_2 - \delta_1 s_1 \end{cases}. \quad (7)$$

Writing $B_j^i = is_j - \varepsilon_j s_j$, $D(i,j) = is_1 - js_2$, $C = \varepsilon_1 s_1 - \varepsilon_2 s_2$ we derive the condition for exact reconstruction of the pair (i, j) as:

$$\max(\delta_2 s_2 - s_1, -\delta_1 s_1) < D(i,j) - C < \min(\delta_2 s_2, -\delta_1 s_1 + s_2). \quad (8)$$

With this reformulation the exact reconstruction property can now be formulated as follows:

for every index j there exists an index i such that $D(i, j)$ satisfies the inequalities in (8).

Next we investigate the conditions on the quantizer parameters for this to hold. To ease discussion we define $L_l = \max(\delta_2 s_2 - s_1, -\delta_1 s_1)$ and $L_r = \min(\delta_2 s_2, -\delta_1 s_1 + s_2)$.

1) As $-\delta_1 s_1 \le \delta_2 s_2$ and $\delta_2 s_2 - s_1 \le -\delta_1 s_1 + s_2$, we have $L_l \le L_r$. Therefore the interval $I = [L_l, L_r]$ is properly defined.
2) Given j, the values of $D(i, j)$ is invariant in i modulo s_1. Therefore, a solution in i exists if and only if $D(i, j) \mod s_1 \in I$.
3) A necessary and sufficient condition for this to hold is that the interval I has size s_1.
4) The interval I has size s_1 if and only if $L_l = \delta_2 s_2 - s_1$ and $L_r = \delta_2 s_2$.
5) This can be re-written as $s_1 \le \delta_1 s_1 + \delta_1 s_2 \le s_2$.

Theorem 1: The exact reconstruction property holds if either

1) $\delta_1 + \delta_2 = 1$ and $s_2 \ge s_1$.
2) $\delta_1 + \delta_2 < 1$ and $s_2 \ge \frac{1-\delta_1}{\delta_2} s_1$.
3) $\delta_1 + \delta_2 > 1$ and $s_2 > \frac{\delta_1}{1-\delta_2} s_1$.

Proof: Case 1 is trivial. Case 2 is proved by observing that the right hand side inequality is automatic and that only the left hand side needs to be enforced. Similar for Case 3, but with left and right reversed. ■

Table I summarizes the three conditions, upon satisfaction of any one of which, the exact reconstruction property is preserved.

For cases of $\delta_1 + \delta_2 \ne 1$, we can further identify the (i, j) pairs that satisfy or fail (8), which indicates whether the exact

Condition	Quantizer	Step size
1	$\delta_1 + \delta_2 < 1$	$s_1 \leq \delta_2 s_2/(1-\delta_1)$
2	$\delta_1 + \delta_2 = 1$	$s_1 \leq s_2$
3	$\delta_1 + \delta_2 > 1$	$s_1 < (1-\delta_2)s_2/\delta_1$

TABLE I

THREE SUFFICIENT CONDITIONS THAT PRESERVE EXACT RECONSTRUCTION PROPERTY.

reconstruction property holds or not respectively. To simplify the discussion, we assume $\varepsilon_1 = \delta_1$. Since i and j are related as $i = \lfloor js_2/s_1 + \delta_1 \rfloor$, we have

$$D = \left\lfloor \frac{js_2}{s_1} + \delta_1 \right\rfloor s_1 - js_2. \tag{9}$$

Given that we only consider cases when $s_1 \leq s_2$, we can set $js_2 = ns_1 + \tau$, where $n, \tau \in \mathbf{Z}^*$ and $\tau \in [0, s_1)$. Considering it as a Diophantine equation with j and n as variables, for it to have integral solutions, τ can only assume values in a subset of $[0, s_1)$, that is, $\Gamma = \{\tau \in [0, s_1) | \text{gcd}(s_1, s_2) \text{ divides } \tau\}$. Eq (9) becomes

$$D = \left\lfloor \frac{\tau}{s_1} + \delta_1 \right\rfloor s_1 - \tau. \tag{10}$$

In the case of $\delta_1 + \delta_2 < 1$, plugging (10) into (8), we have

$$-\delta_2 s_2 \leq \left\lfloor \frac{\tau}{s_1} + \delta_1 \right\rfloor s_1 - \tau \leq \delta_1 s_1. \tag{11}$$

There are only two possibilities for the rounding term. First, if $1 \leq \tau/s_1 + \delta_1 < 2$, it can be derived that τ has to be in the region $(1-\delta_1)s_1 \leq \tau < s_1$. Second, if $0 < \tau s_1 + \delta_1 < 1$, it can be derived that τ has to be in the region $0 \leq \tau \leq \delta_2 s_2$. Joining these two regions, the range T of τ that satisfies (8) is

$$T = \{\tau \in \Gamma | 0 \leq \tau \leq \delta_2 s_2 \ \cup \ (1-\delta_1)s_1 \leq \tau < s_1\}. \tag{12}$$

Equivalently, the range of τ that fails (8) is

$$\tilde{T} = \{\tau \in \Gamma | \delta_2 s_2 < \tau < (1-\delta_1)s_1\}. \tag{13}$$

Apparently, Condition 1 in Table I leads to empty $\tilde{T}$ and is sufficient to preserve the exact reconstruction property.

In the case of $\delta_1 + \delta_2 > 1$, following the same derivation , τ needs to fall into the set T below to satisfy (8)

$$T = \{\tau \in \Gamma | 0 < \tau < (1-\delta_1)s_1 \cup s_1 - (1-\delta_2)s_2 < \tau < s_1\}. \tag{14}$$

And τ needs to fall into the $\tilde{T}$ below to fail (8)

$$\tilde{T} = \{\tau \in \Gamma | (1-\delta_1)s_1 \leq \tau \leq s_1 - (1-\delta_2)s_2\}. \tag{15}$$

Again, Condition 3 in Table I leads to empty $\tilde{T}$ and is sufficient to preserve the exact reconstruction property.

It is easily seen that these sets are determined given any defined $\mathbf{Q}_1$ and $\mathbf{Q}_2$. The identification of these sets makes it possible for us to relax the conditions of exact reconstruction given a particular source content. In particular, the exact reconstruction property is preserved as long as $\tilde{T}$ is empty. Some of the examples will be shown shortly in Section III. We next discuss some specific cases.

D. Discussion on Specific Cases

In JPEG compression, we have $\varepsilon_1 = \delta_1 = 1/2$. To preserve the exact reconstruction property, the authentication quantizer is chosen as $\varepsilon_2 = \delta_2 = 1/2$. This is the result presented in [2], which represents a special case of Theorem 1.

In general image/video compression, ε and δ may be selected from $[0, 1)$ and $(0, 1)$, respectively, based on rate-distortion considerations. For example, MPEG-1/2/4 recommends $\varepsilon_1 = 0, \delta_1 = 1/2$ for quantizers of inter frames. In this case, we know from Theorem 1 that the only quantizer we can select for authentication that resistants to quantization with any $s_1 \leq s_2$, is the one with $\delta_2 = 1/2$. Note that since $\varepsilon_1 \neq \delta_1$ the choice of s_1 is subject to the additional condition $\delta_1 s_1 \in \mathbf{Z}$. In another example, H.264 recommends that for quantizer of intra frames $\varepsilon_1 = \delta_1 = 1/3$ and for inter frames $\varepsilon_1 = \delta_1 = 1/6$. From Theorem 1 it follows that only one quantizer can be chosen for each case, viz. the one with $\varepsilon_2 = \delta_2 = 2/3, 5/6$, respectively.

III. EXPERIMENTAL RESULTS

The experiments are based on the system shown in Figure 1 with $\mathbf{Q}_1$ and $\mathbf{Q}_2$ mapping to $\mathbf{Q}_e$ and $\mathbf{Q}_a$ respectively. Source coefficients x are from a Laplacian distribution. In compression practice, only integral reconstruction levels are used. Whenever $\varepsilon_1 \neq \delta_1$, often times a rounding-down is used at the inverse quantizer. However, this rounding affects the exact reconstruction condition. To avoid this complication, we assume $\varepsilon_1 = \delta_1$, which guarantees that there is no rounding at the inverse quantizer. We will use this setup in all the experiments. We also use a fixed $s_2 = 16$, the step size for the quantizer used in authentication, and consider all coefficients that are eligible for authentication, that is, all the coefficients that are quantized to non-zero values by Q_2. We compute the percentage of these coefficients that preserve the exact reconstruction property.

First we look at a specific case with fixed $s_1 = s_2 - 1$. Figure 2 shows that 100% exact reconstruction happens only for the case that $\delta_1 + \delta_2 = 1$. To further investigate whether the above is true for all $s1 \leq s_2$, we plot the cases with fixed δ_1 and varying δ_2 in Figure 3. We see that for all cases of $s_1 \leq s_2$, 100% exact reconstruction is achieved only when $\delta_1 + \delta_2 = 1$. For all other cases when $\delta_1 + \delta_2 \neq 1$, there are always cases of s_1 that the exact reconstruction property is not preserved.

Inspecting a specific case of $\delta_1 + \delta_2 < 1$, we refer to Figure 3(b) when $\delta_1 = \delta_2 = 1/3$. We know from Table I that the maximum s' that preserves the exact reconstruction for all $s_1 \leq s'$ is $\delta_2 s_2/(1-\delta_1) = 8$. However, we observe that exact reconstruction also holds at $s_1 = 9, 12$. For $s_1 = 9$, we know from (13) that τ needs to be in $(16/3, 6)$ to fail the exact reconstruction test. However, there is no integer in that region, thus making $s_1 = 9$ also preserving the exact reconstruction property. For $s_1 = 12$, we know from (13) that τ needs to be in $(16/3, 8)$ to fail the exact reconstruction test. The region includes two integers, 6 and 7. However, $\text{gcd}(s_1, s_2) = \text{gcd}(12, 16) = 4$ does not divide either 6 or

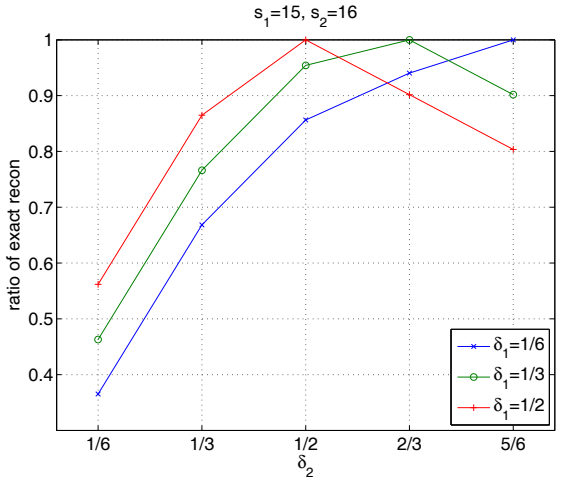


Fig. 2. Ratio of coefficients that achieve exact reconstruction ($\varepsilon_1 = \delta_1$).

7, leading to empty Γ. This also makes $s_1 = 12$ preserving the exact reconstruction property.

Inspecting another specific case of $\delta_1 + \delta_2 > 1$, we refer to Figure 3(a) when $\delta_1 = 1/2, \delta_2 = 2/3$. We know from Table I that the maximum s' that preserves the exact reconstruction for all $s_1 \leq s'$ is $\lceil (1-\delta_2)s_2/\delta_1 \rceil = 11$. However, we observe that exact reconstruction property also holds at $s_1 = 12$. For $s_1 = 12$, we know from (15) that τ needs to be in $[6, 6\frac{2}{3}]$ to fail the exact reconstruction test. The region includes one integer 6, which has been shown before that leads to empty Γ and thus preserves the exact reconstruction property.

IV. Conclusion

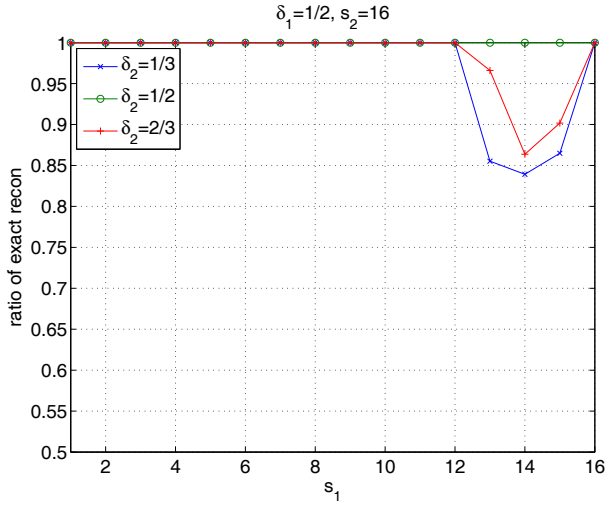
We have proposed in this paper a more general guidance on quantizer selection for authentication. For cases that are applicable to H.264 intra and inter quantization, we find the only workable quantizer for authentication is $\varepsilon_2 = \delta_2 = 2/3, 5/6$, respectively. We have identified the range of s_1 that can preserve exact reconstruction in the cases of $\delta_1 + \delta_2 \neq 1$. For cases when exact reconstruction does not hold, we have also identified the set of coefficient values that fails the exact reconstruction test. This provides alternative selections of $\mathbf{Q}_2$ (the quantizer used for authentication) when there are different considerations on the tradeoff between the authentication capability and the degree of resistance to quantization-based compression. Experimental results have verified all the findings from the analysis.

References

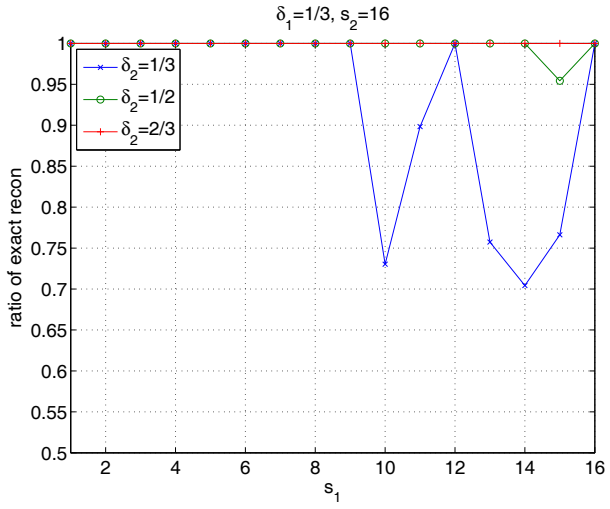
[1] O. Ekici, B. Sankur, B. Coskun, U. Naci, and M. Akcay, "Comparative evaluation of semifragile watermarking algorithms," *Journal of Electronic Imaging*, vol. 13, no. 1, pp. 209–216, Jan. 2004.

[2] C-Y. Lin and S-F. Chang, "Semi-fragile watermarking for authentication jpeg visual content," *Proc. SPIE Security and Watermarking of Multimedia Contents*, pp. 140–151, 2000.

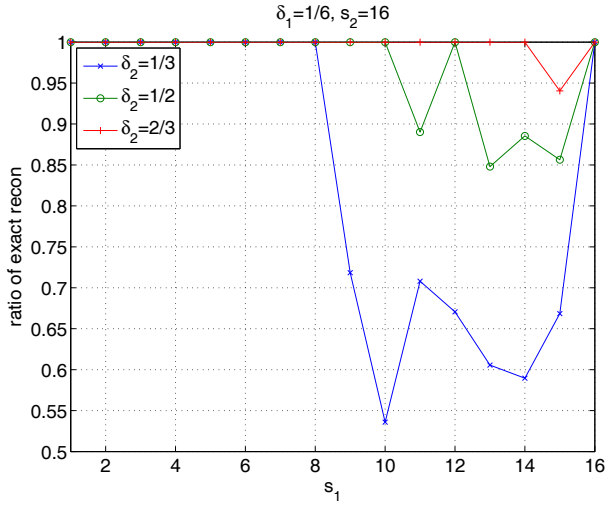
[3] Q. Sun, D. He, and Q. Tian, "A secure and robust authentication scheme for video transcoding," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 16, no. 10, pp. 1232–1244, Oct. 2006.



(a)



(b)



(c)

Fig. 3. Ratio of coefficients that achieve exact reconstruction ($\varepsilon_1 = \delta_1$).