Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **4**, October **2014**

Alternative Syndrome-Trellis Codes With Reduced Trellis Complexity

Wei-Wei Liu, Guang-Jie Liu and Yue-Wei Dai

Department of Automation
Nanjing University of Science and Technology
200 XiaoLingWei, XuanWu District, NanJing, China
lwwnjust5817@gmail.com; gjieliu@gmail.com; daiywei@163.com

Received March, 2014; revised May, 2014

Abstract. *As the state-of-the-art matrix embedding scheme, syndrome-trellis codes (STCs) have been widely used in the field of data hiding. In this paper, for conditions that the cover length is not integral multiple of message length, we give an alternative form of STCs based on quasi convolutional codes, the parity-check matrix of which only consists of single submatrix while that of STCs contains two ones. Experimental results show that the proposed scheme can realize less trellis complexity while achieving similar performance with STCs for these conditions.*
Keywords: Steganography, Syndrome-trellis codes, Quasi convolutional codes, Trellis complexity

1. **Introduction.** As an important branch of information hiding techniques, steganography is mainly applied to covert communication by concealing the very existence of information in some digital medium, such as image, audio, video etc. An effective steganographic scheme aims to embed as much as payload with the distortion as little as possible, which is the problem of so called minimizing embedding impact. Error correcting codes have been widely used for information hiding in two aspects: secret message protection and syndrome coding. The former concentrates on robustness enhancement of the embedded data, in [1, 2], BCH codes and repeat accumulate codes are employed to enocode the embedded data for resisting active-attacks or channel disturbance respectively. While the latter places emphasis on solving the impact minimization problem. Syndrome coding, also known as matrix embedding [3], an embedding method with the cover coefficients perturbed minimally, generally makes the embedded data fall in a coset of the adopted error correcting code. Many steganographic schemes based on this model have been proposed using different types of codes. The first one was constructed by using the family of binary Hamming codes [3], and based on it, the famous steganographic software F5 [4] was developed. Then, many schemes based on the same model have been proposed, they were based on different types of codes: Golay codes [5], BCH codes [6, 7, 8], random linear codes [9], convolutional codes [10, 11]. Among them, syndrome-trellis codes (STCs) [10, 11] is the state-of-the-art one, it is implemented by the Viterbi algorithm [12] on the syndrome trellis structure of convolutional codes and can be capable of performing close to the bounds derived from appropriate rate-distortion bounds. It was adopted as the core algorithm in the famous steganographic tool-HUGO [13] because of its outstanding performance.

As we know, the Viterbi algorithm can be used on most trellis structure directly and convolutional codes have a natural trellis structure. A syndrome trellis is utilized for

trellis-coded quantization in STCs, which can be adaptively constructed by the relative payload. For most relative payloads (except the reciprocal of the integer, e.g., 1/2,1/3), the corresponding parity-check matrices are composed of two types of submatrices. In fact, there exists an alternative form of STCs for these relative payloads based on quasi convolutional codes, the parity-check matrix of which only consists of single type of submatrix.

In this paper, based on the defined quasi convolutional codes and the construction of the corresponding syndrome trellis, an alternative form of STCs is presented. A comparison of the two schemes(STCs and the proposed scheme, which is named QSTCs) for embedding efficiency and the trellis complexity is given, which can report the performance of the two syndrome-trellis-coded quantitative schemes fairly, for some relative payloads, the proposed scheme can achieve reduced trellis complexity.

The whole paper is organized as follows. In Section 2, brief introduction of syndrome-trellis codes for minimizing additive distortion is given. In Section 3, we define a family of quasi convolutional codes with parity-check matrices and present the construction of the corresponding syndrome trellises, which can also be used for the implemention of the Viterbi algorithm. Then, an all-around comparison of the two trellis-coded quantitative schemes with some related experimental results is given in Section 4. Section 5 draws the conclusions.

2. **Syndrome-Trellis Codes For Minimizing Additive Distortion.** Without loss of generality, assume the cover vector $\mathbf{X} \in \{0,1\}^n$ is the binary vector obtained via some bit-assignment operation on the cover object such as mod 2. The stego vector is written as the binary vector $\mathbf{Y} \in \{0,1\}^n$. Assume x_i is changed to y_i for all $i \in \{1,2,...,n\}$. The cost of changing x_i to y_i is defined as $d_i = f(\mathbf{X}, y_i)$, where $d_i \in [0,\infty]$ is the single-letter distortion and may be different for the different x_i despite that $|x_i - y_i|$ always is either 0 or 1. In [10], the single-letter distortion is defined with a relatively simple form as $d_i = \rho_i(x_i \oplus y_i)$. Here, ρ_i is commonly viewed as the single-letter distortion weight. The set of single-letter distortion weight is called the distortion profile which is represented by $\rho = \{\rho_1, ..., \rho_n\}$. And, the total additive distortion function has the below form.

$$D(\mathbf{X}, \mathbf{Y}) = \sum_{i=1}^{n} \rho_i \cdot (x_i \oplus y_i) \tag{1}$$

Suppose the message vector $\mathbf{M} \in \{0,1\}^m$, for matrix embedding, the embedding and extraction mapping are usually realized via a binary linear code $C(n,k)$ with $n-k=m$. Given $\mathbf{H} \in \{0,1\}^{m\times n}$ the parity check matrix of the linear code $C(n,k)$, the embedding and extraction mapping of matrix embedding is commonly written as Eq. (2) and Eq. (3) respectively.

$$Embed : \mathbf{Y} = \text{argmin}_{\varpi \in \{\beta | \mathbf{H}\beta = \mathbf{M}, \beta \in \{0,1\}^n\}} D(\mathbf{X}, \varpi) \tag{2}$$

$$Extract : \mathbf{M} = \mathbf{H}\mathbf{Y} \tag{3}$$

In [10], Filler and Fridrich gave a detailed description of syndrome-trellis codes. They began with constructing the parity-check matrix $\mathbf{H} \in \{0,1\}^{m\times n}$ of convolutional codes. When the cover length is the integral multiple of message length, that is, the relative payload is $\alpha = 1/N$ and N is an integer, the parity-check matrix is obtained by placing a small submatrix $\hat{\mathbf{H}}$ of size $h \times N$, which is placed next to each other and shifted down by one row along the main diagonal , where the parameter h is the memory degree length of the corresponding convolutional code.

However, for most conditions, the reciprocal of the relative payload α is not an integer, we concentrate on these situations in this paper, then the parity-check matrix $\mathbf{H} \in$

$\{0,1\}^{m\times n}$ is composed of two types of submatrices $\hat{\mathbf{H}}_1 \in \{0,1\}^{h\times N}$ and $\hat{\mathbf{H}}_2 \in \{0,1\}^{h\times(N+1)}$ which are uniformly woven with a certain proportion, where $N = \lfloor 1/\alpha \rfloor$, $\lfloor\cdot\rfloor$ means the largest integer smaller than the value.

Assume that the block numbers of $\hat{\mathbf{H}}_1$ and $\hat{\mathbf{H}}_2$ in the parity-check matrix are $block1$ and $block2$ respectively, then they should satisfy that:

$$block1 + block2 = m \tag{4}$$

$$N \cdot block1 + (N+1) \cdot block2 = n \tag{5}$$

which means the proportion of the two submatrices is

$$block1 : block2 = (N + 1 - 1/\alpha) : (1/\alpha - N) \tag{6}$$

e.g., for the relative payload $\alpha = 2/3$ and the memory degree length $h = 3$, the structure of the parity-check matrix $\mathbf{H}$ is shown in FIGURE.1.

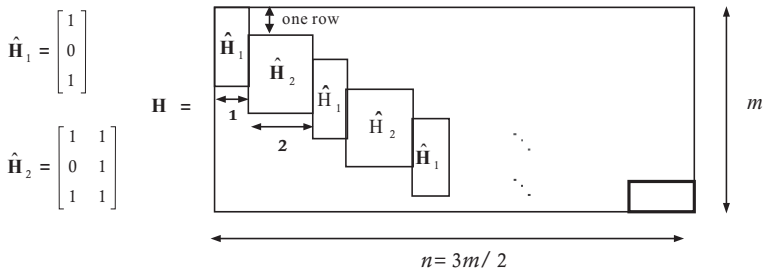

FIGURE 1. Structure of the parity-check matrix for $\alpha = 2/3$ and $h = 3$

The syndrome trellis is parameterized by the embedding message $\mathbf{M} \in \{0,1\}^m$ and can represent members of arbitrary coset $\delta(\mathbf{M}) = \{\mathbf{Z} \in \{0,1\}^n | \mathbf{HZ} = \mathbf{M}\}$. The syndrome trellis is a graph consisting of m trellis blocks, each trellis block corresponds to a submatrix, if the corresponding submatrix is $\hat{\mathbf{H}}_1 \in \{0,1\}^{h\times N}$, the trellis block contains $(N+1)\cdot 2^h$ nodes which are organized in a grid of $N+1$ columns and 2^h rows. The nodes in every column are called states, e.g., the syndrome trellis constructed by the parity-check matrix in FIGURE.1 is shown in FIGURE.2, s_i denotes the i-th message bit.

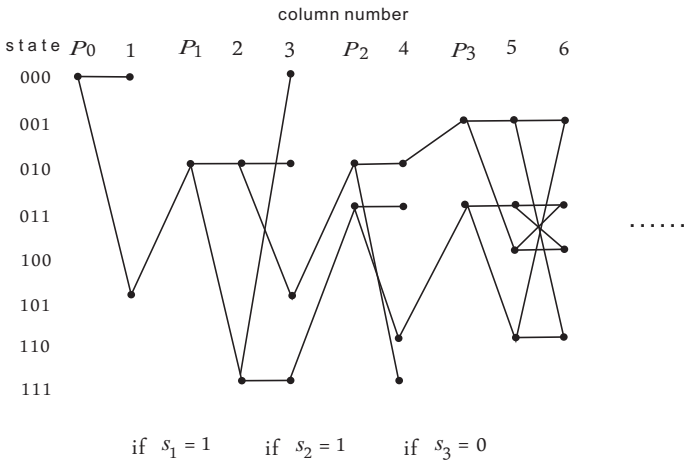

FIGURE 2. Example of syndrome trellis corresponding to FIGURE.1

In STCs, each $\mathbf{Z}$ satisfying $\mathbf{HZ} = \mathbf{M}$ represents a path through the syndrome trellis. Each path starts in the leftmost all-zero state in the trellis and extends to the right. The

path indicates the step-by-step calculation of the syndrome using more and more bits of $\mathbf{Z}$. For example, the first two edges in FIGURE.2, that connect the state 000 from column p_0 with states 000 and 101 in the next column, correspond to label 0 and 1 respectively. At the end of the first block, all paths for which the first bit of the partial syndrome does not match s_1. Then, a new column of the trellis is obtained as the starting column of the next block. With the assigned trellis edges weights, the Viterbi algorithm [9] is used to find the optimal stego object.

3. Syndrome-Trellis Codes Based on Quasi Convolutional Codes.

3.1. **Definition of the quasi convolutional codes.** In this section, we define a family of quasi convolutional codes by parity-check matrix $\tilde{\mathbf{H}}(t)$ with Eq.(7). h denotes the memory degree length, $g(i,j) \in \{0,1\}$, $i \in \{1,...,h\}$, $j \in \{1,...,N\}$.

$$\tilde{\mathbf{H}}(t) = \begin{bmatrix} g(1,1) & \cdots & g(1,N) & & & & \\ \vdots & \ddots & \vdots & & & & \\ g(b_1,1) & \cdots & g(b_1,N) & & & & \\ g(b_1+1,1) & \cdots & g(b_1+1,N) & g(1,1) & \cdots & g(1,N) & \\ \vdots & \ddots & \vdots & \vdots & & \vdots & \\ g(h,1) & \cdots & g(h,N) & g(b_2,1) & \ddots & g(b_2,1) & \\ & & & \vdots & & \vdots & \ddots \\ & & & g(h,1) & \cdots & g(h,N) & \\ & & & & & & \ddots \end{bmatrix} \tag{7}$$

Where $1 \le b_i < h$, $i \in \{1,2,...,t\}$, the submatrix $\hat{\mathbf{H}} = \{g(i,j)\}$ is sized $h \times N$ and the code rate $R = 1 - \sum_{i=1}^{t} b_i/(Nt)$, for syndrome coding, the corresponding relative payload $\alpha = \sum_{i=1}^{t} b_i/(Nt)$. Here, to ensure the embedding performance, we assume $b_i \in \{1,2\}$, $block_1$ denotes the number of submatrices corresponding to $b_i = 1$ and $block_2$ denotes that corresponding to $b_i = 2$. Then we have that

$$block_1 : block_2 = (2/N - \alpha) : (\alpha - 1/N) \tag{8}$$

Where $N = \lceil 1/\alpha \rceil$, $\lceil \cdot \rceil$ means the smallest integer greater than the value.

3.2. **Syndrome trellis driven by quasi convolutional codes.** In order to describe the syndrome trellis with algebraic expression, in the trellis, each state is assigned with a binary h-tuple, e.g., when $h = 3$, the top state in each column is assigned with (000). Each edge $e_{i,j}$ is assigned with $(init(e_{i,j}), fin(e_{i,j}), \lambda(e_{i,j}))$, $init(e_{i,j})$ and $fin(e_{i,j})$ denote the leaving state and arriving state of the edge respectively, $\lambda(e_{i,j}) \in \{0,1\}$ is the label of the edge. If $\mathbf{M} = (s_1,...,s_l)^T$ is the binary message and $\mathbf{E}_1 = (e_{1,1},...,e_{1,N},e_{2,1},...,e_{2,N},...,e_{t,N})$ is a path through the syndrome trellis constructed by $\tilde{\mathbf{H}}(t)$ and $\mathbf{M}$, $l = \sum_{i=1}^{t} b_i$, the message vector $\mathbf{M}$ is first divided into t subvectors $\mathbf{M}_i = \left[s_{\left(\sum_{k=1}^{i} b_k\right)}, ..., s_{\left(1+\sum_{k=1}^{i-1} b_k\right)} \right]$, $i \in \{1,...,t\}$. $e_{i,j}$ represents the j-th edge in the i-th block. Then, the syndrome trellis of the quasi

convolutional code can be represented by Eq.(9)-Eq.(13).

$$\text{fin}(e_{i,j}) = \text{init}(e_{i,j}) \oplus \text{Metric}\,(i,j) \tag{9}$$
$$\text{fin}(e_{i,j}) = \text{init}(e_{i,j+1}) \tag{10}$$
$$\text{R}_{b_i}\left(\text{fin}\left(e_{i,N}\right)\right) = \mathbf{M}_i \tag{11}$$
$$\text{init}\left(e_{i+1,1}\right) = \left[\text{fin}\left(e_{i,N}\right) \oplus s_i\right] \gg b_i \tag{12}$$
$$\text{init}(e_{1,1}) = 0 \tag{13}$$

Where $\text{Metric}\,(i,j) = [\lambda(e_{i,j}) \cdot (g\,(h,j)\,, \cdots, g\,(1,j))]$, "$\oplus$" means bitwise xor, and "$\gg b_i$" means non cyclical right shift b_i bits, e.g. $(1110) \gg 2 = (11)$, function "$\text{R}_{b_i}(\mathbf{X})$" returns the rightmost b_i bits of $\mathbf{X}$, e.g., $\text{R}_2\,(101) = (01)$. With Eq. (9) and Eq. (10), we know that

$$\text{fin}\left(e_{i,N}\right) = \text{init}\left(e_{i,1}\right) \oplus \sum_{j=1}^{N} \text{Metric}\,(i,j) \tag{14}$$

Then, according to Eq. (12), we have

$$\text{init}\left(e_{i+1,1}\right) = \left[\mathbf{M}_i \oplus \text{init}\left(e_{i,1}\right) \oplus \sum_{j=1}^{N} \text{Metric}\,(i,j)\right] \gg b_i \tag{15}$$

From Eq. (11) and Eq. (13), Eq. (16) and Eq. (17) can be obtained.

$$\text{R}_{b_i}\left\{\left(\text{init}\left(e_{i,1}\right)\right) \oplus \sum_{j=1}^{N} \text{Metric}\,(i,j)\right\} = \mathbf{M}_i \tag{16}$$
$$\text{init}\left(e_{i,1}\right) = \sum_{k=1}^{i-1}\sum_{j=1}^{N} \lambda(e_{k,j}) \cdot \left(g\,(h,j) \cdots g\left(1 + \sum_{r=k}^{i-1} b_k, j\right)\right) \tag{17}$$

With Eq. (16) and Eq. (17), we have

$$\begin{aligned}\left(\sum_{k=1}^{i-1}\sum_{j=1}^{N} \lambda(e_{k,j}) \cdot \left(g\left(\sum_{r=k}^{i} b_k, j\right) \cdots g\left(1 + \sum_{r=k}^{i-1} b_k, j\right)\right)\right) \\ \oplus \sum_{j=1}^{N} \left[\lambda(e_{i,j}) \cdot (g\,(b_i,j)\,, ..., g\,(1,j))\right] = \mathbf{M}_i\end{aligned} \tag{18}$$

Thus,

$$\tilde{\mathbf{H}}\,(t) \cdot \lambda\,(\mathbf{E}_1) = \mathbf{M} \tag{19}$$

where $\lambda\,(\mathbf{E}_1) = (\lambda(e_{1,1}), ..., \lambda(e_{1,N}), \lambda(e_{2,1}), ..., \lambda(e_{2,N}), ..., \lambda(e_{t,N}))^T$, it indicates that each path through the syndrome trellis can represent a member of arbitrary coset $\delta\,(\mathbf{M}) = \left\{\mathbf{Z} \in \{0,1\}^n | \tilde{\mathbf{H}}\,(t)\,\mathbf{Z} = \mathbf{M}\right\}$, e.g., for the relative payload $\alpha = 2/3$ and the memory degree length $h = 3$, the proposed syndrome trellis is shown in FIGURE.3.

4. **A Comparison of the Two Trellis-Coded Quantitative Schemes.** As the proposed scheme is also a syndrome-trellis coding scheme, in this section, we give an overall comparison of the two trellis-coded quantitative schemes (STCs and the proposed QSTCs) from the two most important aspects: the trellis complexity and the embedding efficiency.

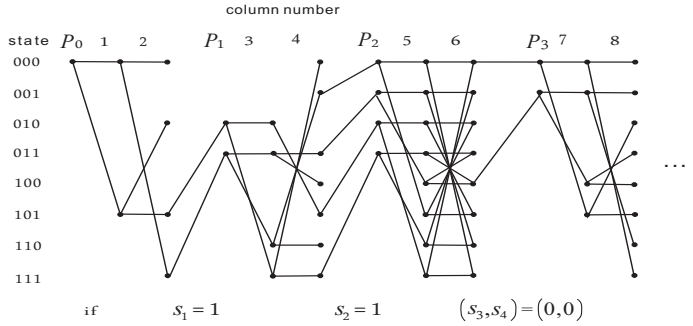

FIGURE 3. Example of the proposed syndrome trellis for $\alpha = 2/3$ and $h = 3$

4.1. **The comparison of trellis complexity.** As we know, the complexity of the trellis-coded quantization is determined by the Viterbi algorithm. In [14], the complexity of Viterbi algorithm was accurately estimated through the number of trellis edge symbols per encoded bit, which was also called the trellis complexity (**TC**) and could be computed from a trellis module. It appears that we can make a fair comparison of the trellis-coded complexity on different trellis structures.

In fact, in these two trellis-coded quantitative schemes, there exist only two types of operations: add operation(**AO**) and comparison operation (**CO**). Each valid edge corresponds one **AO** and when two edges arrive at the same vertex, one **CO** is needed. Thus, the **AO** and the **CO** per encoded bit can be computed as the trellis complexity. We concentrate on the conditions that the reciprocal of the relative payload α is not an integer

For a syndrome trellis module with block length N, $\mathbf{E}(i)$ represents the set of edges which connects the states at the depth $i-1$ and i, where $i = 1, 2, ..., N$ and $|\mathbf{E}(i)|$ denotes corresponding cardinality. If the number of starting states in the first column is γ (the accumulated distortion of the other $2^h - \gamma$ states are all set to $+\infty$), then we have

$$\begin{cases} |\mathbf{E}(i)| \le \gamma \cdot 2^i & i = 1, ..., 1 + h - \lceil \log_2 \gamma \rceil \\ |\mathbf{E}(i)| \le 2 \cdot 2^h & i = 2 + h - \lceil \log_2 \gamma \rceil, ..., N \end{cases} \tag{20}$$

In each trellis module of STCs, $\gamma \le 2^{h-1}$, thus the bounded numbers of (**AO**) and (**CO**) per encoded bit can be obtained according to Eq. (6).

$$\begin{cases} NUM_{STC}^{AO} \le (4 - 2 \cdot \alpha) / (1 - \alpha) \cdot 2^{h-1} \\ NUM_{STC}^{CO} \le (4 - 2 \cdot \alpha) / (1 - \alpha) \cdot 2^{h-2} \end{cases} \tag{21}$$

And for the proposed QSTCs, we have $\gamma \le 2^{h-1}$ for trellis module with corresponding parameter $b_i = 1$ and $\gamma \le 2^{h-2}$ for that with parameter $b_i = 2$, thus we can compute the bounded numbers of (**AO**) and (**CO**) per encoded bit for QSTCs according to Eq. (8).

$$\begin{cases} NUM_{QSTC}^{AO} \le (4 + 1/N - 3 \cdot \alpha) / (1 - \alpha) \cdot 2^{h-1} \\ NUM_{QSTC}^{CO} \le (4 + 1/N - 3 \cdot \alpha) / (1 - \alpha) \cdot 2^{h-2} \end{cases} \tag{22}$$

Where $N = \lceil 1/\alpha \rceil$. With Eq. (21) and Eq. (22), we know that the bounded trellis complexity of the proposed QSTCs is less than or equal to that of STCs as $\alpha \ge 1/N$.

We compute the trellis complexity of two schemes with memory degree length $h = \{6, 8\}$ and relative payload $\alpha = \{2/9,\ 3/10,\ 2/5,\ 3/5,\ 4/5,\ 9/10\}$, the parity-check matrices are all constructed from the brute-force searched submatrices in [10]. The experimental results are shown in FIGURE.4. Each point is plotted by reciprocal relative payload on

the horizontal axis and the number of operations per encoded bit (including **AO** and **CO**) on the vertical axis.

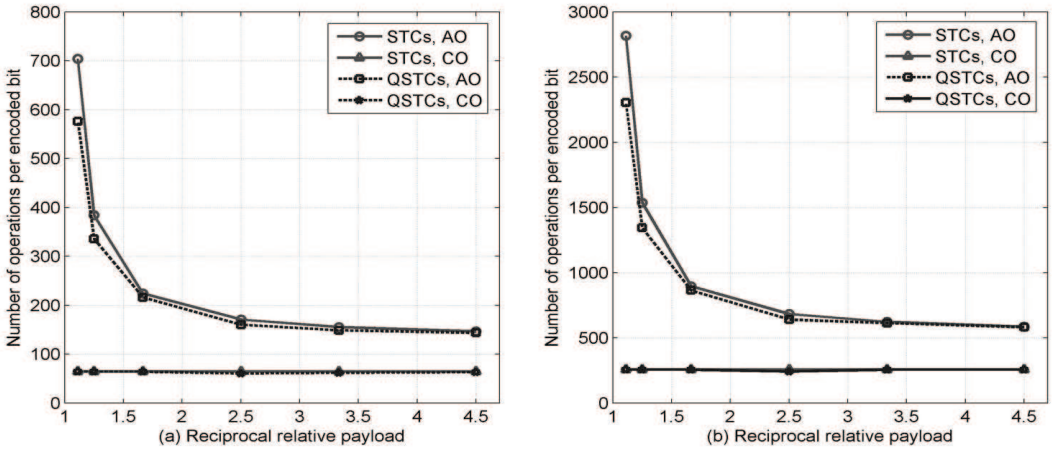

FIGURE 4. (a) The number of operations per encoded bit for $h = 6$, (b) The number of operations per encoded bit for $h = 8$

As shown in above figures, we know that the **AO** per encoded bit of the proposed scheme is obviously less than that of STCs for relative payload , and the **CO** per encoded bit of the two schemes are similar, which means the proposed QSTCs can achieve less trellis complexity than STCs for some relative payloads. Then, we download the C++ source code of STCs from http://dde.binghamton.edu/download/syndrome/. The proposed QSTCs are also implemented on Visual C++ 2008 and optimized with Streaming SIMD Extensions instructions. With the same steganographic configuration as FIGURE.4, and the cover length is fixed to $n = 10^6$, the cover vector and the secret message are both generated by a pseudo-random bits generator, then the running time of the two trellis-coded quantitative schemes are shown in FIGURE.5, the results are obtained using an Intel Core I3 CPU machine utilizing a single CPU core, each point is obtained as an average over 1000 samples, the results of running time are consistent with the comparison results of trellis complexity in FIGURE.4, which reports that the complexity of trellis-coded quantitative scheme can be evaluated by the **AO** and **CO**) per encoded bit and the proposed QSTCs can achieve less trellis complexity than STCs for some relative payloads.

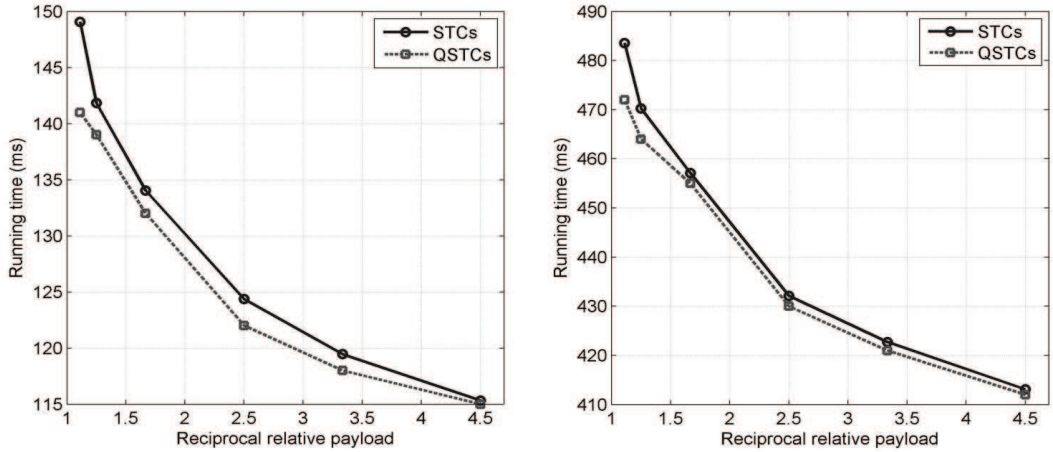

FIGURE 5. (a) Running time for $h = 6$, (b) Running time for $h = 8$

4.2. **The comparison of embedding efficiency.** According to [10], the embedding schemes with a high embedding efficiency on the constant profile exhibit high embedding efficiency for other profiles. Thus in order to make the comparison for embedding performance, we compute the embedding efficiency of two schemes with constant profile in memory degree length $h = \{6, 8, 10\}$ and relative payload $\alpha = \{2/9,\ 3/10,\ 2/5,\ 3/5,\ 4/5,\ 9/10\}$. The cover vector $\mathbf{X} \in \{0,1\}^n$ and the embedding message $\mathbf{M} \in \{0,1\}^m$ are both provided by a pseudo-random bits generator. The code length is fixed to $n = 10^4$, and the embedding efficiency is obtained as an average over 1000 samples. The results are shown in FIGURE.6. Each point is plotted by reciprocal relative payload on the horizontal axis and embedding efficiency on the vertical axis.

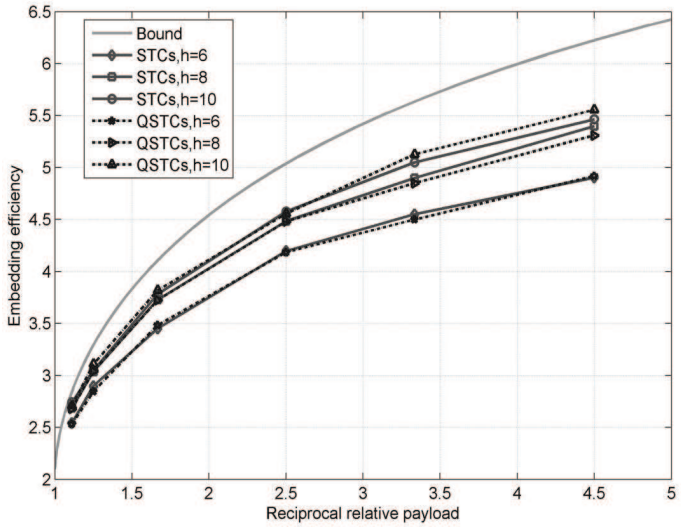

FIGURE 6. Embedding efficiency of the two schemes

FIGURE.6 shows that the embedding efficiency of two schemes are almost the same, they are both capable of performing close to the bounds derived from appropriate rate-distortion bounds, which is consistent with the truth that the proposed QSTCs can be viewed as an alternative constructing scheme of STCs without loss of performance while the trellis complexity is less than STCs for some relative payloads.

5. **Conclusions.** As the first trellis-coded quantitative scheme in steganography, STCs is the state-of-the-art matrix embedding scheme because of the successful utilization of the Viterbi algorithms on the syndrome trellis that is constructed from the parity-check matrix of the convolutional code. In this paper, with an alternative scheme of STCs based on a family of quasi convolutional codes, we give an overall comparison of the two trellis-coded quantitative schemes from the aspects of trellis complexity and embedding efficiency, which indicates that the proposed one can achieve reduced trellis complexity for some relative payloads.

However, as only convolutional codes have a natural trellis structure, there still exist less trellis-coded quantitative schemes in steganography, it is necessary to consider the trellis-coded quantization based on more efficient linear codes, which needs the further studies in the future work.

Acknowledgment. This study was supported by NSF of Jiangsu province (Grant no. BK2010484), and NSF of China (Grantno.61170250, 61103201).

REFERENCES

[1] H. C. Huang, W. C. Fang and S. C. Chen, Copyright protection with EXIF metadata and error control codes, *International Conference on Security Technology,Security Technology, IEEE*, pp. 133-136, 2008.

[2] A. Sarkar, U. Madhow, B. S. Manjunath, Matrix embedding with pseudorandom coefficient selection and error correction for robust and secure steganography, *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 2, pp. 225-239, 2010.

[3] R. Crandall, Some notes on steganography, *Posted on steganography mailing list*, 1998.

[4] A. Westfeld (eds.), F5a steganographic algorithm, *LNCS 2137, Springer*, pp. 289-302, 2001.

[5] M. V. Dijk, F. Willems, Embedding information in grayscale images, *Proc. of the 22nd Symposium on Information and Communication Theory in the Benelux, Enschede, The Netherlands*, pp. 147-154, 2001.

[6] D. Schonfeld, A. Winkler, Embedding with syndrome coding based on BCH codes, *Proc. of the 8th ACM workshop on Multimedia and security*, pp. 214-223, 2006.

[7] R. Zhang, V. Sachnev and H. J. Kim, Fast BCH syndrome coding for steganography, *LNCS 5806, Springer*, pp. 48-58, 2009.

[8] M. O. Medeni, E. M. Souidi, A novel steganographic protocol from error-correcting codes, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 1, pp. 337-343, 2010.

[9] C. Wang, W. Zhang and J. Liu (eds.), Fast matrix embedding by matrix extending, *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 1, pp. 346-350, 2012.

[10] T. Filler, J. Judas, J.Fridrich, Minimizing embedding impact in steganography with trellis-coded quantization, *Proc of SPIE, Electronic Imaging, Media Forensics and Security XII*, pp. 5-14, 2010.

[11] T. Filler, J.Fridrich, Minimizing additive distortion in steganography using syndrome-trellis codes, *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 3, pp. 920-935, 2011.

[12] A. Viterbi, Error bounds for convolutional codes and an asymptotically optimum decoding algorithm, *IEEE Trans. on Information Theory*, vol. 13, no. 2, pp. 260-269, 1967.

[13] T. Pevny, T. Filler, P. Bas, *Using high-dimensional image models to perform highly undetectable steganography, LNCS 6387, Springer*, pp. 161-177, 2010.

[14] K. J. Hole, A comparison of trellis modules for binary convolutional codes, *IEEE Trans. on Communications*, vol. 46, no. 10, pp. 1245-1249, 1998.