StegoNote: Steganography in Guitar Music Using Note Modulation

Hui Tian[1], Zhaohua Zhu[1], Chin-Chen Chang[2], Yongfeng Huang[3], Tian Wang[1], Yonghong Chen[1], and Yiqiao Cai[1]

(Corresponding author: Hui Tian)

College of Computer Science and Technology, National Huaqiao University[1]
Xiamen 361021, China
Department of Information Engineering and Computer Science, Feng Chia University[2]
Taichung 40724, Taiwan
Department of Electronic Engineering, Tsinghua University[3]
Beijing, 100084, China
(Email: cshtian@gmail.com)

(Received May 20, 2018; Revised and Accepted Sept. 22, 2018; First Online July 16, 2019)

Abstract

Due to its diversity, sensual and physical redundancies, music is considered as a type of ideal carrier for steganography, and has attracted increasing attention from the research community of information hiding. In this paper, we present a novel note-modulating steganographic scheme for guitar music. Differing from the existing works, the proposed scheme conceals secret messages into guitar accompaniments based on the fact that there are many note combinations available for expressing a group of similar harmony effects. Specifically, the proposed scheme first determines the available tones for information hiding, and then embeds the secret messages by modulating the note combination of each candidate tone with matrix embedding strategies. The embedding process has no appreciable impact on the playing effect of the music, because only a small part of the musical tones in an accompaniment are substituted by the other note combinations that can achieve similar harmony effects. The proposed scheme is further evaluated with thirty guitar-music samples collected from the Internet. The experimental results demonstrate that the proposed scheme is feasible and efficient. Particularly, employing an appropriate matrix embedding strategy, the proposed scheme can achieve a good balance between steganographic transparency and capacity.

Keywords: Guitar Music; Information Hiding; Music Steganography; Note Modulation

1 Introduction

Steganography is the art and science of concealing secret messages into normal carriers without imperceptible changes [19]. In contrast with cryptographic techniques that aim to protect the content of secret messages [11, 23, 34, 36], it focuses on hiding the very existence of the messages. Therefore, to an extent, steganography can render better security for communications [27], and have thereby attracted increasing attention from various research communities. So far, lots of research works on steganography have been carried out, and the candidate carriers have been also on the increase [39]. Almost all digital media (*e.g.*, image [2, 3, 6, 9, 10, 20, 21, 24, 28, 29, 32, 33], video [16, 38], audio [4, 37], text [12, 14], and Internet protocol [13, 15]) can be considered as steganographic carriers. In this paper, we focus on the steganography on music, which, compared with the existing steganographic techniques on traditional carriers, is largely unexplored but promising.

As is well known, music is a ubiquitous art for people to express their mood, emotion and feeling [31], which has various types and styles. The diversity of music provides an excellent condition for steganography. Moreover, for music, there are both sensual and physical redundancies, making the embedding of secret messages feasible. Specifically, for the same music, different people have diverse feelings, so a slight change will not attract the notice of people; moreover, both melody and harmony can be modulated to hide secret messages while achieving specific music effects. Therefore, the music can be considered as a type of ideal carrier for steganography. It is worth pointing out that, music steganography is different from audio steganography, since the former aims to conceal secret message into the musical content while the latter embeds the secret message into audio signals.

Recently, music steganography has also attracted increasing attention. Generally, the existing works regard-

ing music steganography can be divided into three categories. The first one modulates the pitches of the notes to hide secret messages. For example, Bach, a well-known German musician, uses a note sequence of B^b - A - C - $B^\#$ in his music to represent his name [7]; Hutchinson [8] proposed a scheme based on note modulation, which assigns musical notes to the letters of the embedded message according to their appearance frequency. It is worth noting that the steganographic music, if containing some inappropriate note modulations, will sound weird [17]. Thus, it is advisable to ascertain the correlations of the notes prior to modulating them for information hiding. The second one modifies the music elements (*e.g.*, duration and loudness of the notes) to conceal secret message, behind which the main idea is to exploit the auditory redundancies of these elements to hide the existence of the information hiding. For example, Adli *et al.* [1] proposed a steganographic method for MIDI files by modifying the loudness parameters for "note on" commands, which can be considered as a loudness-modulating method; Moreover, the authors pointed out that the repeated and exclusive commands can be also used to embed secret messages; In addition, Yamamoto *et al.* [35] proposed an adaptive steganographic approach to embed the secret message by modulating the duration of notes; Szczypiorski [25] designed a new steganographic scheme for club music, which embeds secret data into music beats in a subtle way. As mentioned above, this type of methods, due to taking advantage of the auditory redundancies of music, can provide good embedding transparency. Surprisingly, however, all the existing schemes focus on the MIDI music files. The third one conceals the secret messages into sheet music. The sheet music is a handwritten or printed form of music notation that employs musical symbols to indicate the musical content, such as pitches, rhythms and chords, whose purpose is to illustrate the performance skills accurately. For a given sheet music (also called music score), people mainly concentrate on its content, but nearly pay no attention to its typesetting style and visual quality. Therefore, the sheet music is an ideal carrier for steganography. For example, Funk *et al.* [5] proposed an information hiding technique for scanned music scores, which is essentially an image-based steganographic method. Of course, we can easily infer that it is also possible to embed secret messages by modulating the typesetting style (*e.g.*, note spacing and note size).

In this paper, we present a novel note-modulating steganography scheme for guitar music. Differing from the existing works, the proposed scheme aims to embed secret messages into guitar accompaniments, *i.e.*, the musical parts providing harmonic support for the melody. Generally, the harmony of music comes from the simultaneous sounding of multiple notes, and involves chord constructions as well as chord progressions. That is, there are many candidate combinations for notes to express a group of similar harmony effects. Thus, we can achieve information hiding by note modulation. Moreover, we introduce the Hamming matrix encoding strategy to further reduce the embedding distortions. To our best knowledge, this is the first steganographic scheme using the Guitar accompaniments. We evaluate the performance of the proposed scheme with thirty guitar-music samples. The results demonstrate that the proposed scheme is feasible and efficient. Particularly, employing an appropriate matrix embedding strategy, the proposed scheme can achieve a good balance between steganographic transparency and capacity.

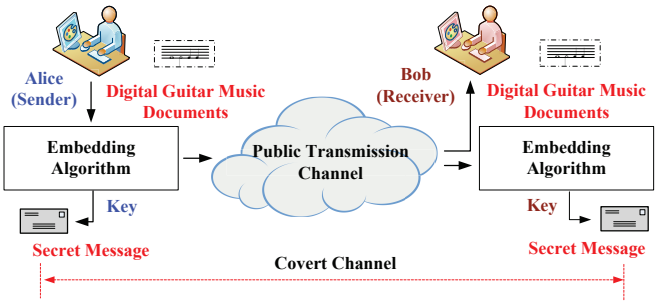


Figure 1: Steganography on music

The rest of this paper is organized as follows. The note-modulating steganographic method for Guitar music is proposed in Section 2, which is followed by evaluation criteria and the experimental results that are presented in Section 3. Finally, we conclude this paper in Section 4.

2 Proposed Scheme

Figure 1 depicts a general framework of steganography on music. Let us assume that Alice as the sender wants to send some secret messages to Bob as the receiver through a public but insecure channel. To achieve this goal, Alice hides secret messages into a piece of music (*e.g.*, guitar music in this paper) using an embedding algorithm, and send the steganographic music to Bob through the public channel; Upon receiving the steganographic music, Bob can obtain secret messages with the corresponding extracting algorithm. In this paper, we present a note-modulating steganographic scheme to achieve steganography on guitar music, which is described as follows.

Assume that Alice wants to send L_M bits of secret messages $M = \{m_i = 0 \ or \ 1 \mid i = 1, 2, \ldots, L_M\}$ to Bob by embedding them into a piece of guitar music Θ. Note that the secret messages are often encrypted prior to embedding, which, however, is independent of the proposed scheme. Thus, we omit the encryption process in this paper, and consider M as the secure form of the given messages for short. Let the accompaniment of the music be $A = \{T_1, T_2, \ldots, T_N\}$, where T_i is the i-th tone, and N is the number of tones in A; Let the chord progression of the music be $\Lambda = \{C_i \mid i = 1, 2, \ldots, L_C\}$, where L_C is the number of the chords in Θ.$C_i = \{c_{i,j} \mid j = 1, 2, \ldots, r_i, 3 \leq r_i \leq 6\}$, $c_{i,j}$ is the j-th

note (chord member) of the i-th chord, and r_i is the number of notes in C_i. In the j-th chord ($j = 1, 2, \ldots, L_C$), let the number of tones be n_j, then the accompaniment can be also denoted as $A = \{\mathcal{T}_j \mid j = 1, 2, \ldots, L_C\}$, where $\Sigma_{j-1}^{L_C} n_j = N$, $\mathcal{T}_1 = \{T_l \mid 1 \le l \le n_1\}$, and $\mathcal{T}_j = \{T_l \mid \Sigma_{k=1}^{j-1} n_k + 1 \le l \le \Sigma_{k=1}^{j} n_k\}$. Accordingly, the embedding process can be described as follows.

Step 1. Decision on available cover tones: With a key K shared by the communication parties, the sender first generates a random binary sequence $S_1 = \{s_{1,j} \mid j = 1, 2, \ldots, N\}$ intended for determining the embedding positions, namely, which tones are chosen to hide information. Note that the random binary sequence S_1 can be also generated according to the desired embedding rate. Assume that the embedding rate is ξ. For each tone, the sender generates a random number $p_j \in [0, 1]$. If $p_j \le \xi$, then $s_{1,j} = 1$; otherwise, $s_{1,j} = 0$. For each tone T_j in the i-th chord, $\Sigma_{k=1}^{i-1} n_k + 1 \le j \le \Sigma_{k=1}^{i} n_k$, we determine the embedding factor λ_j as

$$\lambda_j = \alpha_j \wedge \beta_j \wedge \gamma_j \wedge s_{1,j}, \tag{1}$$

where "$\wedge$" means the AND operation; if T_j is the first tone of the i-th chord, $\alpha_j = 0$, otherwise, $\alpha_j = 1$; if the number of notes involved in T_j is equal to r_i, then $\beta_j = 0$, otherwise, $\beta_j = 1$; if T_j contains the notes not belonging to the i-th chord C_i, then $\gamma_j = 0$, otherwise, $\gamma_j = 1$. If $\lambda_j = 1$, T_j is available for hiding information; otherwise, it cannot be used. For ease of description, we denote the set of all available cover tones as $B = \{b_1, b_2, \ldots, b_{L_B}\}$.

Step 2. Matrix embedding: In our scheme, we employ the Hamming matrix encoding strategy (MES) [26, 30] to achieve information hiding with the minimum distortion. Assume that B is divided into U parts with a length of y shared by the communication parties, namely, $B = \{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_U\}$, where $\mathcal{B}_i = \{\mathfrak{b}_{i,1}, \mathfrak{b}_{i,2}, \ldots, \mathfrak{b}_{i,y}\}$, $i = 1, 2, \ldots, U$, $U = \lfloor L_B/y \rfloor$, $\mathfrak{b}_{i,j} = b_{((i-1)\times y+j)}$, $j = 1, 2, \ldots, y$. Note that, using MES, z bits of secret messages can be embedded into 2^z–1 bits of cover with no more than 1-bit change. That is, for each tone part $\mathcal{B}_i$, $z = \lfloor \log_2(y+1) \rfloor$ bits of secret messages can be embedded. If $y \ge y' = 2^z$–1, we only use the first y' tones in each tone part $\mathcal{B}_i$ as the cover. In this paper, we denote the adopted MES as MES (y', z) for short. Accordingly, M is divided into V parts, namely, $M = \mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_V$, where $\mathcal{M}_i = \mathfrak{m}_{i,1}, \mathfrak{m}_{i,2}, \ldots, \mathfrak{m}_{i,z}$, $i = 1, 2, \ldots, V$. $V = \lfloor L_M/z \rfloor$, $m_{i,j} = m_{((i-1)\times z+j)}$, $j = 1, 2, \ldots, z$. Note that V should be not more than U so that all the secret messages can be embedded. That is to say, the maximum embedding capacity is $z \times U$. For each tone part $\mathcal{B}_i$, the embedding process with MES can be described as follows:

Step 2.1: For $\mathcal{B}_i$, determine the state vector $W_i = \{w_{i,1}, w_{i,2}, \ldots, w_{i,y'}\}$, where

$$w_{i,j} = g(\mathfrak{b}_{i,j}) \ MOD \ 2, j = 1, 2, \ldots, y'. \tag{2}$$

In Equation (2), $g(\mathfrak{b}_{i,j})$ is the sequence number of $b_{i,j}$ in the set of all possible note combinations for the i-th chord. Let the number of notes in $b_{i,j}$ be t. Then, the number of all note combinations is $\mathcal{C}_{r_i}^t$. Table 1 shows all note combinations and their sequence numbers for various values of t and r_i. Note that the sequence numbers of tones in each set can be also randomly assigned to further enhance the security.

Step 2.2: Assign the dependencies with the binary coding of j to $w_{i,j}$; consider each binary coding to be a column vector $D_j = (d_{j,1}, d_{j,2}, \ldots, d_{j,z})^T$, where

$$j = \sum_{k=1}^{z} d_{j,k} \times 2^{(k-1)}. \tag{3}$$

The encoding matrix $\mathbf{D}$ consists of all these vectors, *i.e.*,

$$\mathbf{D} = (D_1, D_2, \ldots, D_{y'}) = \begin{bmatrix} d_{1,1} & d_{2,1} & \cdots & d_{y',1} \\ d_{1,2} & d_{2,2} & \cdots & d_{y',2} \\ \vdots & \vdots & \cdots & \vdots \\ d_{1,z} & d_{2,z} & \cdots & d_{y',z} \end{bmatrix} \tag{4}$$

Step 2.3: For each row in $\mathbf{D}$, calculate

$$x_{i,k} = \begin{cases} 0 & m_{i,k} = \oplus_{j=1}^{y'}(w_{i,j} \times d_{j,k}) \\ 0 & m_{i,k} \ne \oplus_{j=1}^{y'}(w_{i,j} \times d_{j,k}) \end{cases}, 1 \le k \le z, \tag{5}$$

where $\oplus_{j=1}^{y'}$ represents continuous XOR operations.

Step 2.4: Calculate the following expression:

$$X_i = \sum_{k=1}^{z} x_{i,k} \times 2^{k-1}. \tag{6}$$

If $X_i = 0$, there are no bits needed to be changed in W_i, which means the cover part $\mathcal{B}_i$ remains unchanged; otherwise, the X_i-th tone in $\mathcal{B}_i$ needs to be modulated. Specifically, the steganographic tone of the X_i-th tone (denoted by $\mathfrak{b}_{i,X_i}^*$) is an element adjacent to $\mathfrak{b}_{i,X_i}$ in the corresponding set of all possible note combinations. If there are two candidate elements for $\mathfrak{b}_{i,X_i}^*$, the sender can randomly choose one to substitute $\mathfrak{b}_{i,X_i}$. Repeat the above operation for each tone in $\mathcal{B}_i$ until all the secret message are embedded.

Note that, to achieve successful covert communication, both the communication parties should agree on the key, the embedding rate, the adopted MES and the length of secret messages to be embedded. In this paper, we assume that the sender can distribute the parameters to the receiver in a secure manner.

Table 1: Note combinations and their sequence numbers for various values of t and r_i

r_i	t	Tones (No.: Note Combination)
3	1	$1:T_1=\{c_{i,1}\};2:T_2=\{c_{i,2}\};3:T_3=\{c_{i,3}\}$.
	2	$1:T_1=\{c_{i,1},c_{i,2}\};2:T_2=\{c_{i,2},c_{i,3}\};3:T_3=\{c_{i,1},c_{i,3}\}$.
4	1	$1:T_1=\{c_{i,1}\};2:T_2=\{c_{i,2}\};3:T_3=\{c_{i,3}\};4:T_4=\{c_{i,4}\}$.
	2	$1:T_1=\{c_{i,1},c_{i,2}\};2:T_2=\{c_{i,2},c_{i,3}\};3:T_3=\{c_{i,3},c_{i,4}\};4:T_4=\{c_{i,1},c_{i,3}\};$ $5:T_5=\{c_{i,1},c_{i,4}\};6:T_6=\{c_{i,2},c_{i,4}\}$.
	3	$1:T_1=\{c_{i,1},c_{i,2},c_{i,3}\};2:T_2=\{c_{i,2},c_{i,3},c_{i,4}\};3:T_3=\{c_{i,1},c_{i,2},c_{i,4}\};$ $4:T_4=\{c_{i,1},c_{i,3},c_{i,4}\};$
5	1	$1:T_1=\{c_{i,1}\};2:T_2=\{c_{i,2}\};3:T_3=\{c_{i,3}\};4:T_4=\{c_{i,4}\};5:T_5=\{c_{i,5}\}$.
	2	$1:T_1=\{c_{i,1},c_{i,2}\};2:T_2=\{c_{i,2},c_{i,3}\};3:T_3=\{c_{i,3},c_{i,4}\};4:T_4=\{c_{i,4},c_{i,5}\};$ $5:T_5=\{c_{i,1},c_{i,3}\};6:T_6=\{c_{i,1},c_{i,4}\};7:T_7=\{c_{i,1},c_{i,5}\};8:T_5=\{c_{i,2},c_{i,4}\};$ $9:T_9=\{c_{i,2},c_{i,5}\};10:T_{10}=\{c_{i,3},c_{i,5}\}$.
	3	$1:T_1=\{c_{i,1},c_{i,2},c_{i,3}\};2:T_2=\{c_{i,2},c_{i,3},c_{i,4}\};3:T_3=\{c_{i,3},c_{i,4},c_{i,5}\};$ $4:T_4=\{c_{i,1},c_{i,2},c_{i,4}\};5:T_5=\{c_{i,1},c_{i,2},c_{i,5}\};6:T_6=\{c_{i,1},c_{i,3},c_{i,4}\};$ $7:T_1=\{c_{i,1},c_{i,3},c_{i,5}\};8:T_8=\{c_{i,1},c_{i,4},c_{i,5}\};9:T_9=\{c_{i,2},c_{i,3},c_{i,5}\};$ $10:T_{10}=\{c_{i,2},c_{i,4},c_{i,5}\}$.
	4	$1:T_1=\{c_{i,1},c_{i,2},c_{i,3},c_{i,4}\};2:T_2=\{c_{i,2},c_{i,3},c_{i,4},c_{i,5}\};3:T_3=\{c_{i,1},c_{i,2},c_{i,3},c_{i,5}\};$ $4:T_4=\{c_{i,1},c_{i,2},c_{i,4},c_{i,5}\};5:T_5=\{c_{i,1},c_{i,3},c_{i,4},c_{i,5}\}$.
6	1	$1:T_1=\{c_{i,1}\};2:T_2=\{c_{i,2}\};3:T_3=\{c_{i,3}\};4:T_4=\{c_{i,4}\};5:T_5=\{c_{i,5}\};$ $6:T_6=\{c_{i,6}\}$.
	2	$1:T_1=\{c_{i,1},c_{i,2}\};2:T_2=\{c_{i,2},c_{i,3}\};3:T_3=\{c_{i,3},c_{i,4}\};4:T_4=\{c_{i,4},c_{i,5}\};$ $5:T_5=\{c_{i,5},c_{i,6}\};6:T_6=\{c_{i,1},c_{i,3}\};7:T_7=\{c_{i,1},c_{i,4}\};8:T_5=\{c_{i,1},c_{i,5}\};$ $9:T_9=\{c_{i,1},c_{i,6}\};10:T_{10}=\{c_{i,2},c_{i,4}\};11:T_{11}=\{c_{i,2},c_{i,5}\};12:T_{12}=\{c_{i,2},c_{i,6}\}.$ $13:T_13=\{c_{i,3},c_{i,5}\};14:T_{14}=\{c_{i,3},c_{i,6}\};15:T_{15}=\{c_{i,4},c_{i,6}\}$.
	3	$1:T_1=\{c_{i,1},c_{i,2},c_{i,3}\};2:T_2=\{c_{i,2},c_{i,3},c_{i,4}\};3:T_3=\{c_{i,3},c_{i,4},c_{i,5}\};$ $4:T_4=\{c_{i,4},c_{i,5},c_{i,6}\};5:T_5=\{c_{i,1},c_{i,2},c_{i,4}\};6:T_6=\{c_{i,1},c_{i,2},c_{i,5}\};$ $7:T_1=\{c_{i,1},c_{i,2},c_{i,6}\};8:T_8=\{c_{i,1},c_{i,3},c_{i,4}\};9:T_9=\{c_{i,1},c_{i,3},c_{i,5}\};$ $10:T_{10}=\{c_{i,1},c_{i,3},c_{i,6}\};11:T_{11}=\{c_{i,1},c_{i,4},c_{i,5}\};12:T_{12}=\{c_{i,1},c_{i,4},c_{i,6}\}.$ $13:T_{13}=\{c_{i,1},c_{i,5},c_{i,6}\};14:T_{14}=\{c_{i,2},c_{i,3},c_{i,5}\};15:T_{15}=\{c_{i,2},c_{i,3},c_{i,6}\}.$ $16:T_{16}=\{c_{i,2},c_{i,4},c_{i,5}\};17:T_{17}=\{c_{i,2},c_{i,4},c_{i,6}\};18:T_{18}=\{c_{i,2},c_{i,5},c_{i,6}\}.$ $19:T_{19}=\{c_{i,3},c_{i,4},c_{i,6}\};20:T_{20}=\{c_{i,3},c_{i,5},c_{i,6}\}$.
	4	$1:T_1=\{c_{i,1},c_{i,2},c_{i,3},c_{i,4}\};2:T_2=\{c_{i,2},c_{i,3},c_{i,4},c_{i,5}\};3:T_3=\{c_{i,3},c_{i,4},c_{i,5},c_{i,6}\};$ $4:T_4=\{c_{i,1},c_{i,2},c_{i,3},c_{i,5}\};5:T_5=\{c_{i,1},c_{i,2},c_{i,3},c_{i,6}\};6:T_6=\{c_{i,1},c_{i,2},c_{i,4},c_{i,5}\};$ $7:T_7=\{c_{i,1},c_{i,2},c_{i,4},c_{i,6}\};8:T_8=\{c_{i,1},c_{i,2},c_{i,5},c_{i,6}\};9:T_9=\{c_{i,1},c_{i,3},c_{i,4},c_{i,5}\};$ $10:T_{10}=\{c_{i,1},c_{i,3},c_{i,4},c_{i,6}\};11:T_{11}=\{c_{i,1},c_{i,3},c_{i,5},c_{i,6}\};$ $12:T_{12}=\{c_{i,1},c_{i,4},c_{i,5},c_{i,6}\};13:T_{13}=\{c_{i,2},c_{i,3},c_{i,4},c_{i,6}\};$ $14:T_{14}=\{c_{i,2},c_{i,3},c_{i,5},c_{i,6}\};15:T_{15}=\{c_{i,2},c_{i,4},c_{i,5},c_{i,6}\}$.
	5	$1:T_1=\{c_{i,1},c_{i,2},c_{i,3},c_{i,4},c_{i,5}\};2:T_2=\{c_{i,2},c_{i,3},c_{i,4},c_{i,5},c_{i,6}\};$ $3:T_3=\{c_{i,1},c_{i,2},c_{i,3},c_{i,4},c_{i,6}\};4:T_4=\{c_{i,1},c_{i,2},c_{i,3},c_{i,5},c_{i,6}\};$ $5:T_5=\{c_{i,1},c_{i,3},c_{i,4},c_{i,5},c_{i,6}\}$.

To illustrate the above embedding process, we give a concrete example, as shown in Figure 2. The set of tone parts is $A=\{T_1,\ T_2,\ \cdots,\ T_{15}\}=\{\mathrm{d}^1,\ \{a^1,\ c^2,\ f^2\},\ a,\ \{a^1,\ c^2\},\ \{a^1,\ c^2\},\ g,\ \{d^1,\ g^1,\ b^1\},\ g,\ \{d^1,\ g^1\},\ \{d^1,\ g^1\},\ c^1,\ \{e^1,\ g^1,\ b^1\},\ g,\ \{g^1,\ b^1\},\ \{g^1,\ b^1\}\}$, the chord progression is $\wedge=\{C_1,\ C_2,\ C_3\}$, where $C_1=\{\mathrm{d}^1,\mathrm{a}^1,\mathrm{c}^2,\mathrm{f}^2,\mathrm{a}^2\}$, $C_2=\{\mathrm{g},\mathrm{d}^1,\ g^1,\mathrm{b}^1,\mathrm{g}^2\}$ and $C_3=\{\mathrm{c}^1,\mathrm{e}^1,\mathrm{g}^1,\mathrm{b}^1,\mathrm{e}^2\}$(marked by blue notes). Hence, we can obtain the embedding factors for the tones in A is {0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1}, because T_1, T_6 and T_{11} are respectively the first tone of corresponding chords, $T3$ and T_{13} contain the notes not belonging to the corresponding chords.

Accordingly, the set of all available cover tones $B=\{T_2,T_4,T_5,T_7,T_8,T_9,T_{10},T_{12},T_{14},T_{15}\}$. Assume that MES (3, 2) is adopted, and B is divided into three parts, *i.e.*,$B=\{\mathcal{B}_1,\mathcal{B}_2,\mathcal{B}_3\}$. For the first part $\mathcal{B}_1=\{T_2,T_4,T_5\}=\{\{\mathrm{a}^1,\mathrm{c}^2,\mathrm{f}^2\},\{\mathrm{a}^1,\mathrm{c}^2\},\{\mathrm{a}^1,\mathrm{c}^2\}\}$ (marked by gray area), the set of the tone states $W_1=\{0,0,0\}$. According to Step 2.3, we can get the encoding matrix as

$$\mathbf{D}=\begin{bmatrix}1&0&1\\0&1&1\end{bmatrix}.$$

Assume the current part of the secret message is $\mathcal{M}_1=\{1,0\}$. According to Equation (5), we get

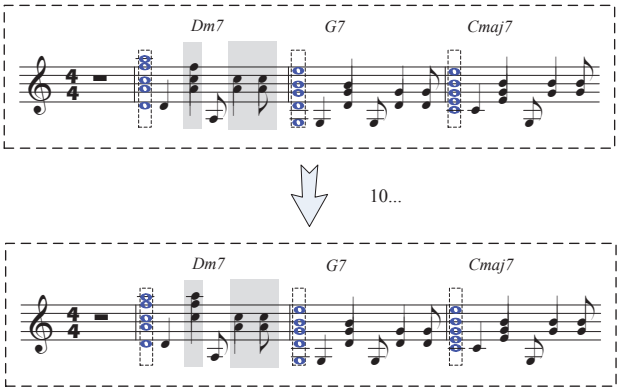


Figure 2: An Example for the Embedding Process of Note-modulating Steganographic Scheme

$x_{1,1} = 1$, $x_{1,2} = 0$. Due to $X_1 = 1 \times 1 + 0 \times 2 = 1$, the first element in W_1 needs to be changed. That is, the first tone in $\mathcal{B}_1$, *i.e.*, T_2, needs to be modulated to an adjacent note combination (*e.g.*, $\{c^2, f^2, a^2\}$) to represent state "1". Therefore, the steganographic version of $\mathcal{B}_1$ is $\{d^1, \{c^2, f^2, a^2\}, a, \{a^1, c^2\}, \{a^1, c^2\}\}$.

The receiver can restitute the secret message M by the following steps:

Step 1. Extraction: With the shared key K and the embedding rate ξ, the receiver first generates the random binary sequence $S_1 = \{s_{1,j} \mid j = 1, 2, \ldots, N\}$, and calculate the embedding factor λ_j as Equation (1). Accordingly, the set of the tones containing secret information can be obtained, denoted as $B^* = \{b_1^*, b_2^*, \ldots, b_{L_B}^*\}$.

Step 2. Decoding: Divide B^* into U parts with y (denote as $B^* = \{\mathcal{B}_1^*, \mathcal{B}_2^*, \ldots, \mathcal{B}_U^*\}$); for the first y' tones in each tone part $\mathcal{B}_i^*$, the receiver calculates the corresponding tone state $W_i^* = \{w_{i,1}^*, w_{i,2}^*, \ldots, w_{i,y'}^*\}$ according to Equation (2), and then get each bit of embedded message by calculating the following expression:

$$\mathfrak{m}_{i,k} = \oplus_{j=1}^{y'}(w_{i,j}^* \times z_{j,k}),\ 1 \le k \le z. \tag{7}$$

Combining all the extracted bits, the receiver can obtain the whole secret message M.

Let the possibility of $\alpha_j = 0$ be P_α, the possibility of $\beta_j = 0$ be P_β, the possibility of $\gamma_j = 0$ be P_γ. Then, the possibility of $\lambda_j = 1$ can be determined as

$$P(\lambda_j = 1) = (1 - P_\alpha - P_\beta - P_\gamma) \times \xi, \tag{8}$$

where $P_\alpha = L_C \,/\, N$; $P_\beta = N_\beta \,/\, N$, N_β is the number of tones whose notes are equal to the number of the notes in the corresponding chords; $P_\gamma = N_\gamma \,/\, N$, N_γ is the number of tones which contain the notes not belonging to the corresponding chords. Note that the three conditions for unavailable tones are judged one by one, so the three sets of unavailable tones have no common elements. Therefore, the capacity of the proposed scheme (denoted by ω) can be determined as

$$\begin{aligned} \omega &= \lfloor \frac{N \times (1 - P_\alpha - P_\beta - P_\gamma) \times \xi}{y} \rfloor \times z \\ &= \lfloor \frac{(N - L_C - N_\beta - N_\gamma) \times \xi}{y} \rfloor \times z. \end{aligned} \tag{9}$$

3 Performance Evaluation

To evaluate the performance of the proposed scheme, we collect thirty pieces of guitar accompanies from the Internet, including three types of music styles, namely, BossaNova, Folk and Popular. For each sample, we perform four kinds of steganographic experiments at the embedding rate of 100%, namely, the steganography with no MES, the ones with MES (3, 2), the one with MES (7, 3) and the one with MES (15, 4). The secret message produced randomly can be successfully embedded and extracted in any case. Table 2 shows the embedding capacities of all the music samples in various steganographic cases. Figure 3 further shows the average embedding capacities per measure for all the music samples in the four steganographic modes, respectively. From them, we can learn the following facts. First, the embedding capacities of all the music samples are identical with the ones calculated as Equation (9), indicating the proposed scheme is feasible and correct. Second, the thirty music samples render different embedding capacity even in the same steganographic mode. The reason for the difference on their capacities is that there are different numbers of tones in each measure. In other words, the average capacity per measure is proportionate to the number of tones in each measure. Therefore, we can choose the samples containing as many tones as possible in each measure for hiding information. For example, the twelfth, nineteenth, twenty-fifth and twenty-ninth music samples are much better than the others in term of embedding capacity.

In addition, we introduce dissonance value [18, 22] and harmony entropy [22], which are popularly applied in the objective evaluation of music, to evaluate the steganographic transparency in terms of the sensory consonance.

Plomp and Levelt [18, 22] pointed out that the dissonance of two single tones can be parameterized by a model as

$$d(x) = e^{-b_1 x} - e^{-b_2 x}, \tag{10}$$

where x denotes the absolute value of the difference in frequency between two single sinusoids, $b_1 = 3.5$ and $b_2 = 5.75$.

According to this definition, the inherent dissonance of the complex tone $F = \{f_i \mid i = 1, 2, \ldots, n\}$ can be calculated as the sum of the dissonances of all pairs of partials, namely,

$$D_F = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} d(f_i, f_j). \tag{11}$$

Table 2: The Statistical result of the ABX tests for different music styles

No.	Music Samples	N	L_C	N_β	N_γ	None	MES(3,2)	Capacity(bit) MES (7,3)	MES(15,4)
1	Autumn leaves[1]	326	66	0	73	187	124	78	48
2	Blue bossa[1]	337	79	0	80	178	118	75	44
3	Cherie sweet honey[1]	416	72	0	82	262	174	111	68
4	Fly me to the moon[1]	303	56	0	65	182	120	78	48
5	Happy birthday[1]	343	58	0	42	243	162	102	64
6	Moon represent my heart[1]	487	82	0	84	321	214	135	84
7	Night swing[1]	278	65	17	110	86	56	36	20
8	Skimming over the surface[1]	433	73	0	108	252	168	108	64
9	The warmest love song[1]	625	105	0	13	507	338	216	132
10	Write a song[1]	553	97	0	106	350	232	150	92
11	Auld lang syne[2]	265	67	0	0	198	132	84	52
12	Childhood memory[2]	545	69	0	0	476	316	204	124
13	Forest birch[2]	607	76	0	277	254	168	108	64
14	Grandma's penghu bay[2]	373	63	0	0	310	286	132	80
15	Katyusha[2]	377	95	0	0	282	188	120	72
16	Lilac[2]	643	81	0	280	282	188	120	72
17	Orchid[2]	229	58	0	0	171	114	72	44
18	Red river valley[2]	261	66	0	65	130	86	54	32
19	Seasons song[2]	289	37	0	0	252	168	108	64
20	Snail and oriole bird[2]	287	54	0	0	233	154	99	60
21	Baby[3]	440	80	0	59	301	200	129	80
22	Can't help falling in love[3]	501	129	0	103	269	178	114	68
23	Crescent moon[3]	558	84	0	172	302	200	129	80
24	I miss you[3]	407	119	1	112	175	116	75	44
25	June rain[3]	516	68	0	0	448	298	192	116
26	Endless story love[3]	472	100	0	2	370	246	156	96
27	Rainbow[3]	566	77	0	243	246	164	105	64
28	Starry mood[3]	524	78	0	150	296	196	126	76
29	T1213121[3]	305	39	0	8	258	172	108	68
30	Wonderful power song[3]	512	104	0	0	408	272	174	108

Note: [1] belongs to the style of BossaNova, [2] belongs to the style of Folk, [3] belongs to the style of Popular.

Further, the dissonance of F at an interval α can be calculated as follows.

$$D_F(\alpha) = D_F + D_{\alpha F} + \sum_{i=1}^{n}\sum_{j=1}^{n} d(f_i, \alpha f_j), \tag{12}$$

where $\alpha F = \{\alpha f_i \mid i = 1, 2, \ldots, n\}$ represents the note of F at an interval α.

Accordingly, the dissonance of a chord of three notes at the intervals 1, a and b can be calculated by adding the dissonances between all partials, namely,

$$D_F(a, b) = D_F(a) + D_F(b) + D_{aF}(b \ / \ a). \tag{13}$$

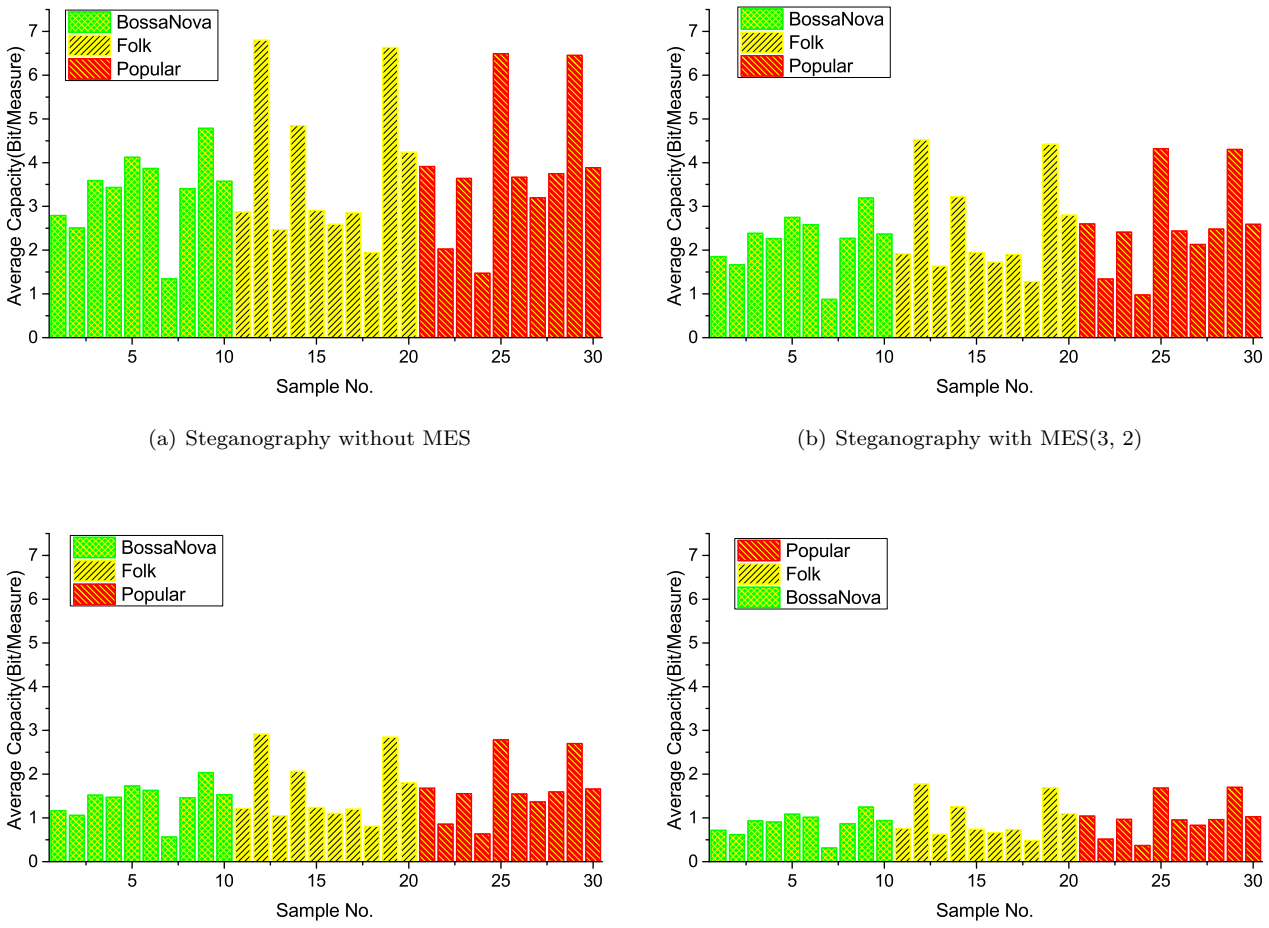
Harmonic entropy is a measure of the uncertainty in pitch perception [23]. When two musical notes are played simultaneously at an interval α, they must have a simple-integer ratio (denoted as f_α) about the frequency, which can be modeled with a Farey series $\mathcal{F}_m$ of an order m. For any interval α, the probability that α is perceived as a mistuning of the j-th member of the Farey series is

$$p_j(\alpha) = \frac{1}{\sigma\sqrt{2\pi}} \int_{t \in r_j} e^{-(t-i)^2/2\sigma^2} dt, \tag{14}$$

where $\sigma = 0.007$, r_j represents the region over which f_j dominates, going from the median below to the median above. Assume that the j-th member of the Farey series is $f_j = c_j \ / \ d_j$, and $r_j \in [(c_{j-1} + c_j) \ / \ (d_{j-1} + d_j), (c_j + c_{j+1}) \ / \ (d_j + d_{j+1})]$. Then the harmonic entropy of α can be defined as

$$HE(\alpha) = -\sum_j p_j(\alpha) \log(p_j(\alpha)). \tag{15}$$

To evaluate the steganographic transparency of the proposed scheme, we randomly choose six music samples and their steganographic versions in different modes to make statistics on the dissonance values and harmony entropy. Figures 4 and 5 show the experimental results of the dissonance values and harmony entropy, respectively. From the charts, we can learn the following fact. First, the



(a) Steganography without MES

(b) Steganography with MES(3, 2)

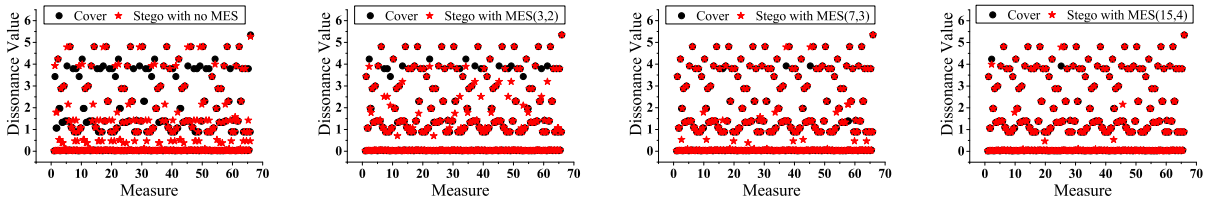
(c) Steganography with MES (7, 3)

(d) Steganography with MES (15, 4)

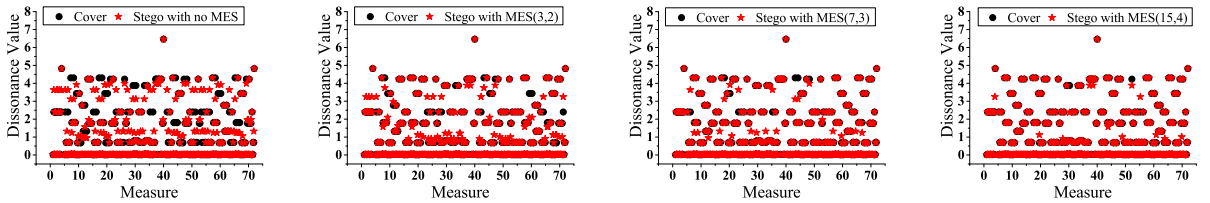
Figure 3: Average steganographic capacity per measure for all the music samples

dissonance values and harmony entropy of some measures are diverse, although all of them are in the normal range. Particularly in the first style, the distributions have a relatively large range, which is caused by various chord types. For example, the major chord, which is a type of consonant chords in music theory, contains a major third and a perfect fifth above its root note. The major seventh chord, which is a dissonant chord, contains a major third, a perfect fifth, and a major seventh. Therefore, the ranges of both dissonance values and harmony entropy for tones in different chords are also different. Second, the dissonance value and harmony entropy of each measure in the steganographic accompaniments for a given music sample, are identical or highly similar to those in the original accompaniments, indicating that the steganographic samples can be played at a good level of sensory consonance. That is, the proposed scheme can achieve good steganographic transparency in term of the sensory consonance. Particularly, as the length of cover part is increased, the embedding distortions are accordingly reduced, namely, better steganographic transparency can be achieved. In this sense, the proposed scheme can achieve a good balance between steganographic transparency and capacity by introducing an appropriate MES.

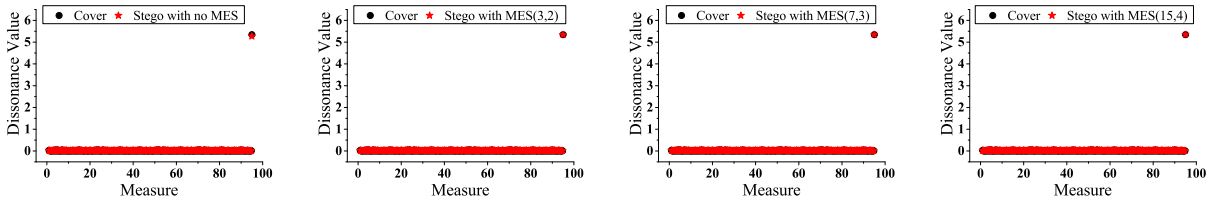
In addition, we also conduct ABX tests to further evaluate the steganographic transparency of the proposed scheme. We create a sample set as X by randomly selecting two original accompaniments and eight steganographic ones (two samples without MES, two samples with MES (3, 2), two samples with MES (7, 3), and two samples with MES (15, 4)) for each style, and invite thirty persons (including ten professionals in the information hiding field, ten guitar lovers and ten common participators) to identify the categories of all the music samples in X independently. Specifically, if a sample is identified as an original one, it is labeled as A; otherwise, it is labeled as B. Table 3 and Table 4 show the statistical results of the ABX tests for different music styles and for different steganographic modes. It is not hard to find out that for any given test set, the participants even the guitar lovers who are familiar with these music styles, cannot accurately distinguish between the original and stegano-



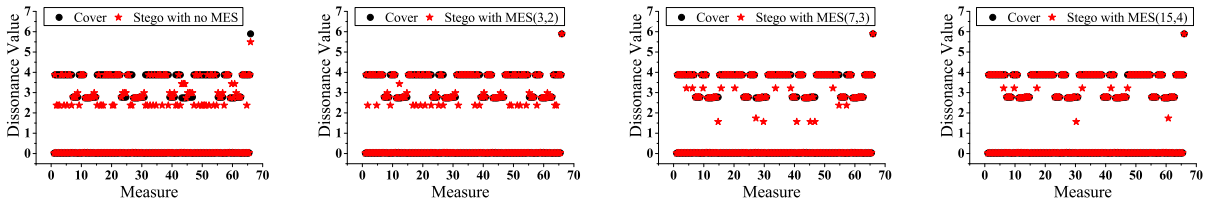
(a) Autumn Leaves



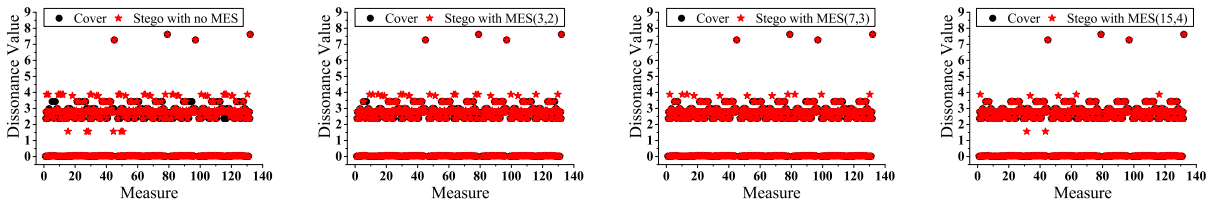
(b) Cherie Sweet Honey



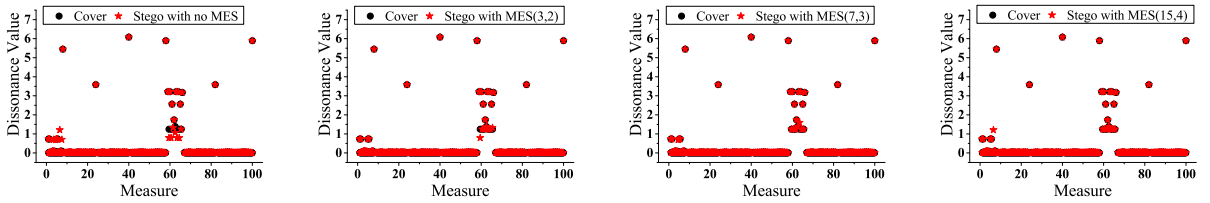
(c) Katyusha



(d) Red River Valley

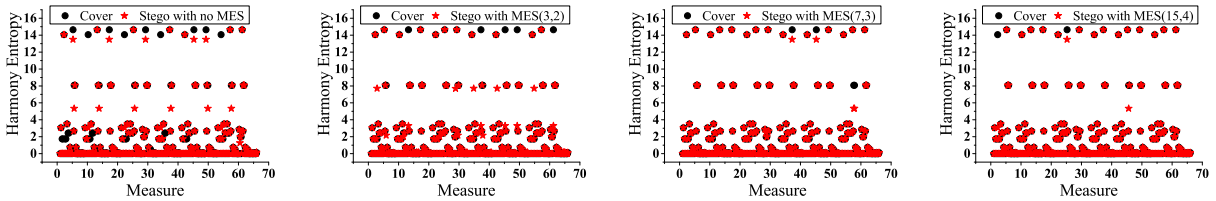


(e) Can't Help Falling In Love

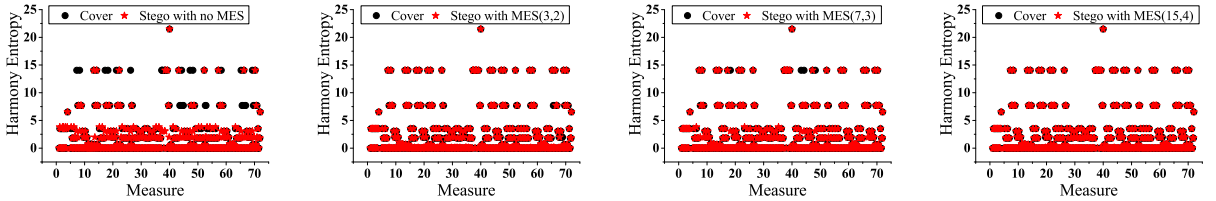


(f) Endless story love

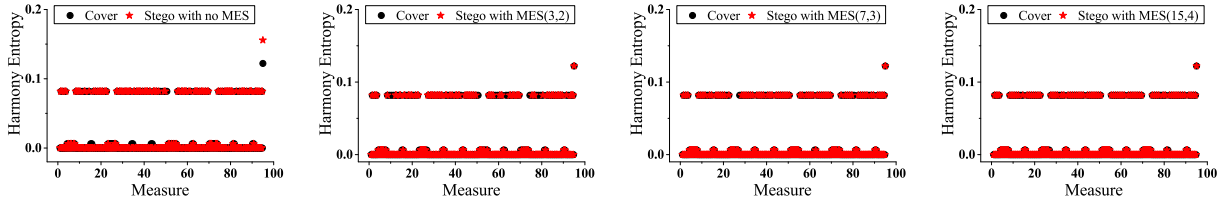
Figure 4: The statistical results for dissonance values



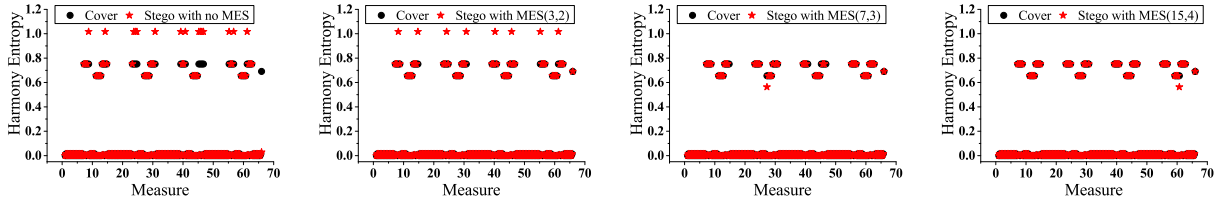
(a) Autumn Leaves



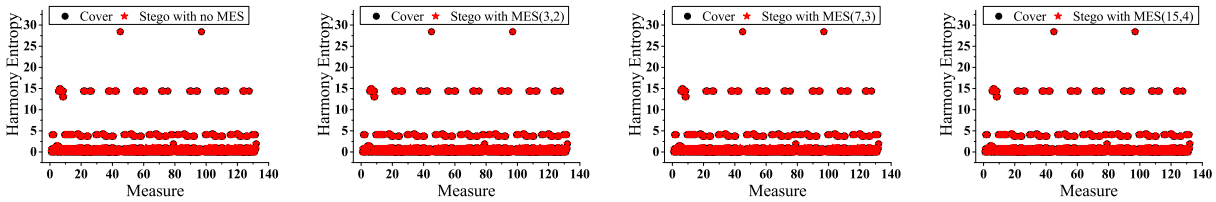
(b) Cherie Sweet Honey



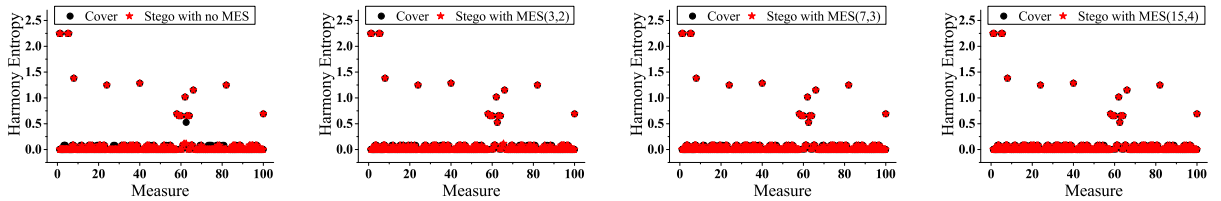
(c) Katyusha



(d) Red River Valley



(e) Can't Help Falling In Love



(f) Endless story love

Figure 5: The statistical results for harmony entropy

Table 3: The statistical result of the ABX tests for different music styles

	Bossa Nova	Folk	Popular
Guitar Lovers	46%	53%	47%
Professionals	42%	48%	61%
Participators	49%	51%	53%

Table 4: The statistical result of the ABX tests for different steganographic modes

	With no MES	With MES (3, 2)	With MES (7, 3)	With MES (15, 4)
Guitar Lovers	60%	53%	53%	52%
Professionals	57%	50%	51%	53%
Participators	48%	49%	46%	53%

graphic samples, which demonstrates again that the proposed scheme can achieve excellent steganographic transparency. Particularly, for the guitar lovers, as the length of cover part is increased, their accuracy for distinguishing the original and steganographic samples is further decreased, which demonstrates again that MES can further improve the steganographic transparency. Moreover, the results also suggest again that the proposed scheme can achieve a good balance between steganographic transparency and capacity by choosing a proper MES.

4 Conclusions

Steganography, which can conceal secret messages into seemingly normal carriers without any perceptible change, provides an efficient means for secure communication. So far, extensive researches on steganography have been carried out, and steganographic covers have been also extended from initial images to almost all multimedia. Due to its diversity, sensual and physical redundancies, music is considered as a type of ideal carrier for steganography, and has attracted increasing attention from the research community of information hiding. In this paper, we present a novel note-modulating steganographic scheme for guitar music. Differing from the existing works, the proposed scheme aims to embed secret messages into guitar accompaniments based upon the fact that there are many note combinations for expressing a group of similar harmony effects. In other words, the proposed scheme conceals the secret messages by suitably modulating the note combinations for the corresponding candidate tones. Additionally, we introduce the Hamming matrix encoding strategy to further reduce the embedding distortions. To our best knowledge, this is the first steganographic scheme using the Guitar accompaniments. We evaluate the proposed scheme with a large number of guitar-music samples. The experimental results demonstrate that the proposed scheme is indeed feasible and efficient. In particular, by introducing an appropriate matrix embedding strategy, the proposed scheme can achieve a good balance between steganographic transparency and capacity.

Acknowledgments

This work was supported in part by National Natural Science Foundation of China under Grant Nos. U1536115 and U1405254, Natural Science Foundation of Fujian Province of China under Grant No. 2018J01093, Program for New Century Excellent Talents in Fujian Province University under Grant No. MJK2016-23, Program for Outstanding Youth Scientific and Technological Talents in Fujian Province University under Grant No. MJK2015-54, Promotion Program for Young and Middle-aged Teacher in Science & Technology Research of Huaqiao University under Grant No. ZQN-PY115 and Program for Science & Technology Innovation Teams and Leading Talents of Huaqiao University under Grant No.2014KJTD13.

References

[1] A. Adli and Z. Nakao, "Three steganography algorithms for midi files," in *Proceedings of the International Conference on Machine Learning and Cybernetics*, pp. 2401–2404, Aug. 2005.

[2] Y. Cao, Z. Zhou, X. Sun, and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Computers, Materials & Continua*, vol. 54, no. 2, pp. 197–207, 2018.

[3] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing*, vol. 90, no. 3, pp. 727–752, 2010.

[4] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2012, no. 1, p. 25, 2012.

[5] W. Funk and M. Schmucker, "High capacity information hiding in music scores," in *Proceedings of the*

First International Conference on Web Delivering of Music, pp. 12–19, Nov. 2001.

[6] L. C. Huang, T. H. Feng, and M. S. Hwang, "A new lossless embedding techniques based on HDWT," *IETE Technical Review*, vol. 34, no. 1, pp. 40–47, 2017.

[7] P. Hunt. "J. S. bach and steganography," *Electrum Magazine*, 2013. (`http://www.electrummagazine.com/2013/12/j-s-bach-and-steganography/`)

[8] L. Hutchinson, "Live musical steganography," *Scholar Commons*, 2014. (`https://scholarcommons.sc.edu/senior_theses/20/`)

[9] B. Jana, "Dual image based reversible data hiding scheme using weighted matrix," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 6–19, 2016.

[10] J. Li, Q. Lin, C. Yu, X. Ren, and P. Li, "A QDCT- and svd-based color image watermarking scheme using an optimized encrypted binary computer-generated hologram," *Soft Computing*, vol. 22, no. 1, pp. 47–65, 2018.

[11] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2201–2210, 2014.

[12] Y. Liu, X. Sun, C. Gan, and H. Wang, "An efficient linguistic steganography for chinese text," in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 2094–2097, July 2007.

[13] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 225–229, 2014.

[14] Y. B. Luo, Y. F. Huang, F.F. Li, and C. C. Chang, "Text steganography based on ci-poetry generation using markov chain model," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 9, pp. 4568–4584, 2016.

[15] W. Mazurczyk, "Voip steganography and its detection—a survey," *ACM Computing Surveys (CSUR'13)*, vol. 46, no. 2, p. 20, 2013.

[16] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A robust and secure video steganography method in dwt-dct domains based on multiple object tracking and ECC," *IEEE Access*, vol. 5, pp. 5354–5365, 2017.

[17] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[18] R. Plomp and W. J. M. Levelt, "Tonal consonance and critical bandwidth," *The Journal of the Acoustical Society of America*, vol. 38, no. 4, pp. 548–560, 1965.

[19] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE security & privacy*, vol. 99, no. 3, pp. 32–44, 2003.

[20] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 4, pp. 636–646, 2016.

[21] S. Rajendran and M. Doraipandian, "Chaotic map based random image steganography using lsb technique.," *International Journal Network Security*, vol. 19, no. 4, pp. 593–598, 2017.

[22] W. A. Sethares, "Consonance and dissonance of harmonic sounds," *Tuning, Timbre, Spectrum, Scale*, pp. 77–95, 2005.

[23] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[24] M. Shobana, "Efficient x-box mapping in stego-image using four-bit concatenation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 29–33, 2014.

[25] K. Szczypiorski, "Stegibiza: New method for information hiding in club music," in *Proceedings of the 2016 2nd International Conference on Frontiers of Signal Processing (ICFSP'16)*, pp. 20–24, Oct. 2016.

[26] H. Tian, H. Jiang, K. Zhou, and D. Feng, "Transparency-orientated encoding strategies for voice-over-IP steganography," *The Computer Journal*, vol. 55, no. 6, pp. 702–716, 2012.

[27] H. Tian, J. Qin, Y. Huang, Y. Chen, T. Wang, J. Liu, and Y. Cai, "Optimal matrix embedding for voice-over-IP steganography," *Signal Processing*, vol. 117, pp. 33–43, 2015.

[28] Y. L. Wang, J. J. Shen, and M. S. Hwang, "An improved dual image-based reversible hiding technique using lsb matching.," *International Journal Network Security*, vol. 19, no. 5, pp. 858–862, 2017.

[29] Y. G. Wang, G. Zhu, and Y. Q. Shi, "Transportation spherical watermarking," *IEEE Transactions on Image Processing*, vol. 27, no. 4, pp. 2063–2077, 2018.

[30] A. Westfeld, "F5—A steganographic algorithm," in *Proceedings of the fourth International Workshop on Information Hiding*, pp. 289–302, 2001.

[31] C. L. Wu, C. H. Liu, and C. K. Ting, "A novel genetic algorithm considering measures and phrases for generating melody," in *Proceedings of the IEEE Congress on Evolutionary Computation (CEC'14)*, pp. 2101–2107, July 2014.

[32] N. I. Wu and M. S. Hwang, "Development of a data hiding scheme based on combination theory for lowering the visual noise in binary images," *Displays*, vol. 49, pp. 116–123, 2017.

[33] N. I. Wu and M. S. Hwang, "A novel LSB data hiding scheme with the lowest distortion," *The Imaging Science Journal*, vol. 65, no. 6, pp. 371–378, 2017.

[34] Z. Wu, B. Liang, L. You, Z. Jian, and J. Li, "High-dimension space projection-based biometric encryption for fingerprint with fuzzy minutia," *Soft Computing*, vol. 20, no. 12, pp. 4907–4918, 2016.

[35] Kotaro Yamamoto and Munetoshi Iwakiri, "A standard midi file steganography based on fluctuation of duration," in *Proceedings of the 2009 International Conference on Availability, Reliability and Security*, pp. 774–77, Mar. 2009.

[36] L. Yang, Z. Han, Z. Huang, and J. Ma, "A remotely keyed file encryption scheme under mobile cloud computing," *Journal of Network and Computer Applications*, vol. 106, pp. 90–99, 2018.

[37] X. Zhang, Y. A. Tan, C. Liang, Y. Li, and J. Li, "A covert channel over volte via adjusting silence periods," *IEEE Access*, vol. 6, pp. 9292–9302, 2018.

[38] Y. Zhang, M. Zhang, X. Yang, D. Guo, and L. Liu, "Novel video steganography algorithm based on secret sharing and error-correcting code for H. 264/avc," *Tsinghua Science and Technology*, vol. 22, no. 2, pp. 198–209, 2017.

[39] E. Zielińska, W. Mazurczyk, and Krzysztof Szczypiorski, "Trends in steganography," *Communications of the ACM*, vol. 57, no. 3, pp. 86–95, 2014.

Biography

Hui Tian received the PhD degree in 2010 in computer science from Huazhong University of Science and Technology, Wuhan, China. He is now a professor and associate dean of the college of computer science and technology, National Huaqiao University, Xiamen, China. His present research interests include network & information security, steganography and steganalysis, digital forensics, and cloud computing security. He has published more than 80 papers in refereed proceedings of conferences, journals and books, and got five patents. He is a senior member of IEEE, a senior member of China Computer Federation (CCF), a member of the Technical Committee on Internet of CCF and a member of the Technical Committee on Information Storage of CCF.

Zhaohua Zhu received the B.Sc degree in computer science and technology in 2015 from National Huaqiao University, Xiamen, China. He is now pursuing the M. Sc. degree in computer science from National Huaqiao University, Xiamen, China. His interests are in the areas of information hiding, with current focus on steganography based on music.

Chin-Chen Chang received both the B.Sc. degree in Applied Mathematics in 1977 and the M.Sc. degree in Computer and Decision Sciences in 1979 from National Tsinghua University, Hsinchu, Taiwan, and the Ph.D. degree in computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. His current title is Chair Professor in department of information engineering and computer science, Feng Chia University, from Feb. 2005. Prior to joining Feng Chia University, he was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. His present research interests include computer cryptography and information security, cloud computing, data engineering and database systems. He has over 850 publications in major journals and international Conferences in these areas. Since his early years of career development, he consecutively won Outstanding Youth Award of Taiwan, Outstanding Talent in Information Sciences of Taiwan, AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of Taiwan, Outstanding Engineering Professor Award of Taiwan, Chung-Shan Academic Publication Awards, Distinguished Research Awards of National Science Council of Taiwan, Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, etc. He is currently a Fellow of IEEE and a Fellow of IEE, UK.

Tian Wang received his PhD degree in computer science in City University of Hong Kong in 2011. Currently, he is a professor in the college of computer science and technology, National Huaqiao University, Xiamen, China. His research interests include wireless sensor networks, fog computing and mobile computing. He has published more than 100 papers in refereed proceedings of conferences and journals. He is a member of IEEE.

Yonghong Chen received the PhD degree in 2005 in automation control engineering from Chongqing University, Chongqing, China. He is now a professor in the college of computer science and technology, National Huaqiao University, Xiamen, China. His present research interests include network and multimedia information security, information hiding and watermarking. He has published over 60 papers in refereed proceedings of conferences and journals.

Yiqiao Cai received the Ph.D. degree in computer science in 2012 from Sun Yat-sen University, Guangzhou, China. He is now an associate professor in the college of computer science and technology, National Huaqiao University, Xiamen, China. His present research interests include differential evolution, multi-objective optimiza-tion, and other evolutionary computation techni-ques. He has published over 40 papers in refereed proceedings of conferences and journals.