Hiding Messages using Musical Notes: A Fuzzy Logic Approach

Kirti Kamalpratap Singh
Master in computer Application
Thakur Institute of Management Studies, Career Development and Research
Mumbai, India

Neelima Ranvijay Singh
Master in computer Application
Thakur Institute of Management Studies, Career Development and Research
Mumbai, India

Pankaj Mudholkar
HoD – MCA
Thakur Institute of Management Studies, Career Development and Research
Mumbai, India

ABSTRACT

"Music words can be used as a communication language". Musical symbols and musical notes have been used as codes and ciphers from early days. Encrypting messages using music is known as Musical cryptography and it uses predefined set of notes and set of rules for creating musical pieces which in turn are musical cryptograms. Traditional algorithms which are applied to musical cryptography used simple substitution cipher which produced good musical sequences. To overcome this problem of fuzzy logic based algorithm for musical cryptography is proposed in this paper. The paper proposes a symmetric key substitution cipher which uses one of the n candidate notes to encrypt a particular character. The application of fuzzy logic in music cryptography produces a acceptable musical sequences which are hard to be finding as cipher

General Terms

Musical Cryptography, musical words, algorithmic composition, fuzzy logic, encryption and decryption techniques.

Keywords

Musical Cryptography, musical words, algorithmic composition, fuzzy logic, encryption and decryption techniques.

1. INTRODUCTION

For secure communication and exchange of information cryptography and steganography have been used. Cryptography is the process of transforming the plain text message into a cipher text which cannot be understood by unknown people. The process of converting plain text message into cipher (decrypted) text is known as encryption, while the process of getting plain (original) text back from cipher text is known as decryption. Various techniques are used to convert the plain text into cipher text. These techniques can be used as simple permutation and combination, transposition, substitution, matrix multiplication etc. For an encryption and decryption techniques usually keys is used, if the same key is used in the cryptography for encryption and decryption the process is known as symmetric key cryptography while two different keys i.e. public and private keys are used know as asymmetric key cryptography. In asymmetric key cryptography the public key is known to everyone who can be used to encrypt the message while the private key remains private to the receiver which is used to decrypt the message. A block cipher algorithm encrypts a particular fixed length size block while a stream cipher encrypts a stream of plain text and can encrypt particular characters at a time. Steganography is the art of hiding messages into another message. Now day's steganography uses digital media as a cover file to hide the respected message also known as payload data. Images, audio, video and executable files are used as cover media. The bits of the cover media is modified as per the bits of intended message. The techniques used for modifying bit are LSB least significant bit substitution, echo hiding, parity bit modification etc. Both steganography and cryptography have advantages and disadvantages over another. The main aim of cryptography is to encrypt the message in a way that the cipher text should not be decrypted without the access of the decryption key and trying all the possible keys should not be feasible. Modern day, cryptography and steganography are used together to solve the problem of message security. Today cryptographic algorithms are considered as the intruder cannot get the plain text message from the cipher text in polynomial time. Modern day's cryptography algorithm addresses the issues of confidentiality, integrity, authentication and non-repudiation.

2. MUSICAL CRYPTOGRAPHY

Musical cryptography uses musical notations, keywords and musical notes to encrypt messages .Musical cryptography is used to encrypt the messages into the musical form. Musical cryptography produces musical cryptography which are normally difficult to be detected as cipher. Music and its attributes have used in cryptography from early days. The simplest way of the musical ciphers used to replace characters of the plain text message with musical notes. The encrypted messages can be in the form of musical symbols, verbal or instrumental musical sequences.

2.1 Abbreviations and Acronyms

MIDI stands for Musical Instrument Digital Interface, it is a standard developed for the communication of musical devices. MIDI is a technical standard that describes a protocol, digital interface and connectors and allows wide variety of electronic musical instruments, computers and other related devices to connect and communicate with one another. MIDI carries an event messages that specify notation, pitch and velocity, control signals for parameters such as volume, vibrato, audio panning and clock signals that set and synchronize tempo multiple devices. These messages are sent via a MIDI cable to other devices where they control sound generation and other features. This data can also be recorded into a hardware or software device called a sequencer, which can be used to edit the data and to play it back at a later time.

A general midi file contains sequences of musical notes, the timing intervals, the control messages etc. A simple musical note can be represented in MIDI as a set of on set, duration, MIDI channel, MIDI note, velocity associated to a particular note in a chronological order of occurrence of events. MIDI notes represent the pitch of the notes; pitch is also called frequency and is represented as the note number in MIDI. MIDI note number ranges from 0 to 127. “D Eb F Fb E F F# G Ab A Bb B” are the 12 chromatic notes used in western music composition whose Indian equivalent is “Sa, re, Re, ga, Ga, ma, Ma, Pa, da, Da, ni, Ni”. An device contains the 12 chromatic notes. Same note played on different device have different frequencies. The relation between the frequencies of notes of two different devices can be described with the temperament. In music all the 16 channels can be used for simultaneous playback of different notes for different instruments. MIDI is capable of handling 10.7 octaves which is generally beyond the limits of the instrument. Velocity tells how soft or loud a particular note will play. Velocity can take value from 0 to 127. MIDI files are best suited for the purpose of musical representation in Algorithmic Composition.

Table 1 .General Midi Data Structure

Onset (Beats)	Duration (Beats)	MIDI channel	MIDI Note	Velocity	Onset (Sec)	Duration (sec)
0.00	1.48	1	50	127	0.00	0.89
1.50	0.98	1	09	127	0.90	0.59
2.50	1.00	1	85	127	1.50	0.60
3.50	0.50	1	64	127	2.10	0.30
4.00	0.98	1	29	127	2.40	0.59
5.00	0.48	1	33	127	3.00	0.29

Recurrent neural networks, rule based grammars, genetic algorithms, fuzzy logic and many others have been employed in musical compositions. These techniques help the composers in composing good musical piece but it’s also helps in reducing the manual efforts in composition of the music and reduces the time required. In this algorithm composition composer is seen as the searcher and all possible musical compositions are considered as search space. The composer tries to reach at nearly possible solution which is in terms of quality musical sequence. Any permutation and combination of musical notes does not produce music. Music composition consists of set of rules and grammar. Algorithmic composition should take care of harmonic and melodic relation between consecutive and concurrent notes. Melody refers to the playback of musical notes in sequence (one after another) in a way which is pleasant to ear. Harmony refers to the concurrent playback of notes which are in consonance to each other. For good understanding of any harmony and the melody. Harmonic and melodic relations are hard to quantify, so use of strict rules and grammars does not provide flexibility in algorithmic composition. Chord progression also plays a big role in music composition. Random occurrence of musical notes is prohibited in music; we can predict the next note to occur provided we have knowledge of the last notes and the transition probabilities of all the other notes. Transition probability is defined as the probability of occurrence of next note provided the previous note was fixed. Transition probability matrix for a particular genre can be deduced from observation of several musical pieces of that genre .A first order Markov chain considers previous outcomes to predict next outcome, while second order Markov chain uses last two outcomes to predict the next outcome.

Table 2 .Transition Probability Matrix For Rag Bilawal

	Sa	Re	Ga	Ma	Pa	Da	Ni
Sa	0.075	0.313	0.161	0	0.048	0.130	0.273
Re	0.475	0	0.460	0.024	0.024	0.017	0
Ga	0	0.267	0.013	0.358	0.362	0	0
Ma	0	0.512	0.464	0	0.024	0	0
Pa	0.010	0	0.010	00.495	0.067	0.410	0.010
Da	0.010	0	0.010	0.052	0.448	0	0.479
Ni	0.343	0.015	0	0	0.015	0.612	0.015

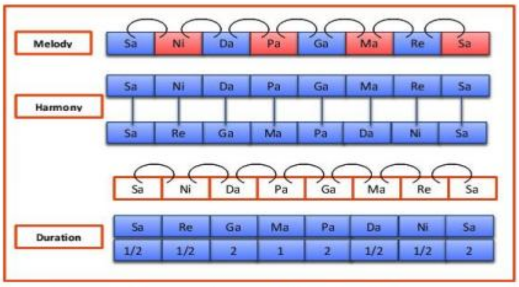
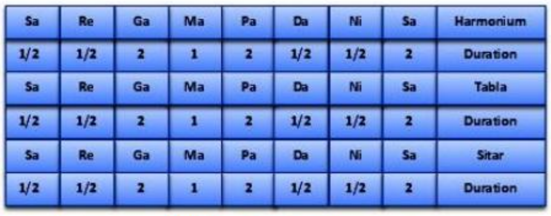


Figure 1. Representation of Melody and Harmony



Sa	Re	Ga	Ma	Pa	Da	Ni	Sa	Harmonium
1/2	1/2	2	1	2	1/2	1/2	2	Duration
Sa	Re	Ga	Ma	Pa	Da	Ni	Sa	Tabla
1/2	1/2	2	1	2	1/2	1/2	2	Duration
Sa	Re	Ga	Ma	Pa	Da	Ni	Sa	Sitar
1/2	1/2	2	1	2	1/2	1/2	2	Duration

Figure 2. Concurrent Playback for Chords of Different Instruments

2.2 Fuzzy Logic

Fuzzy logic is used to formalize the human capacity of approximate reasoning by using fuzzy sets and fuzzy relations. The classical set theory defines the behavior of an object as either belonging or not in a particular set. In classical set theory the boundaries of the set are real valued. The classical definition of the sets fails in linguistic classification, e.g. hot, cold, short, medium and tall. We cannot define a real valued boundary for the class short or tall, neither it fits for the case of hot or cold. In these cases fuzzy sets are used, in fuzzy sets every member has a grade of membership in the set. The membership value ranges from 0 to 1, where zero means no participation and 1 means full participation, the values between 0 and 1 means partial participation. Classical set operations such as ‘and’ and ‘or’ between two fuzzy sets are realized using the minimum and maximum of the membership values of the two sets respectively. Fuzzy rules are used for approximate reasoning. Fuzzy rules are used in musical composition for the harmonization and orchestration of musical sequences. A particular chord can be harmonized using the fuzzy rules. In this proposed work a particular window size (say of n notes) is taken which will be harmonized depending on the melodic structures of the chord and candidate notes. The fitness value of the generated sequence can be calculated using the weighted sum of the transition probabilities of the notes in the particular window and the fuzzified membership for the melodic and harmonic aesthetic of the sequence. The genesis rules will be defined depending on the genre of musical composition chosen. These genesis rules will synthesize and sequence the musical notes to yield an optimal musical pattern. Rules for the note density, pitch range and repeated rhythmic values will be used to make the musical composition as realistic as possible. The relative note density is the proportion of notes and rests and the repeated rhythmic value is the proportion of melodic interval in which both notes have the same rhythmic value. Some of the general rules derived from the musical theory and compositions of various performers can be listed as below :

Melodic Rule:

A Chord should start and end with a tonic.

- Leaps along the notes should not be higher than two octaves.
- A step wise motion of at least half of the melodic interval should be present.
- Melodic consonance should be present and dissonant notes should be avoided.

Harmonic Rules:

- Parallel octaves should be avoided.
- Parallel fifths should be avoided.
- Consonance and dissonance should be considered.

Rhythm rules:

- Note duration of each type should be present from eighth note to full note.
- Same note should not repeat more than thrice.

Harmonic intervals:

- Perfect consonance: 1,5,8
- Imperfect consonance: 3,6
- Dissonance: 2,4,7

Melodic Intervals:

- Perfect Consonance: 1,5,8
- Imperfect consonance: 3,4,6
- Dissonance: 2,7

The fuzzy rules for the melody, harmony, step size can be defined with the membership mharmony, mmelody, mstepsize.

The overall system function of the fuzzy logic block can be defined as

M=mharmony(interval).mmelody(interval).mstepsize(interval)*transition_prob(notes)

mharmony(interval) is the membership function for the Harmonyof the chord. (refer Figure 5) mmelody(interval) is the membership function for melody of the chord. (refer Figure 6) mstepsize(interval) is the membership function for the step size rules. The membership value for stepsize is either 1 or 0. Transition probability of the chord is weighted sum of transition probabilities of notes in the chord.

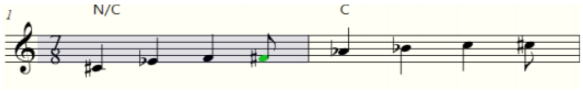


Figure 3. Notation of Chord "Sa re ga ma pa da ni sa"

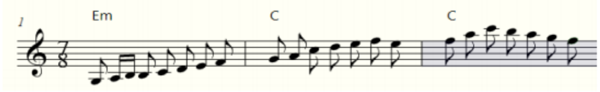


Figure 4. Relative Step Size of One for Two Consecutive Notes

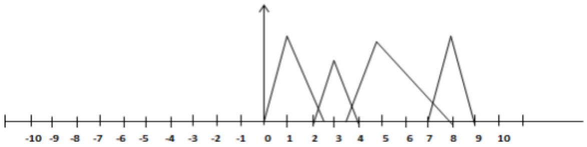


Figure 5. m_harmony

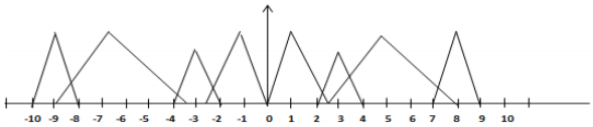


Figure 6. m_melody

Key Matrix and Genesis Rules Let C={c1, c2, …….., cn} be the character set which is used to write the plaintext message and N={n1,n2,n3,…………..nn} be the note set, where the features of ni can be denoted as fni={MIDI pitch, channel number, velocity, tempo}. The MIDI pitch and channels together will produce a note set of length 128x16, which can be used for encoding 2048 different letters into musical notes, provided we are using a simple replacement/ substitution of particular letter with single note. In the proposed work the algorithm encodes a particular character into one of the m candidate notes. Which can be written as candidate_notes(Ci)={nm1, nm2,…, nmn}. This representation will mean that a particular character can be encoded by one of the several candidate notes, while one particular note can represents only one character. If n is the length of character set, then m should be chosen such that nxm <= 2048. The value 2048 represents the maximum possible length of the note set. If the length of character set is higher, then the number of candidate notes will be lesser. In that case we will encrypt each byte of data individually, that means character set is reduced to a manageable length of 256 and the number of candidate notes will be 8. The encryption and decryption key consists of an nxm matrix where n rows will correspond to n characters of the character set and each row will have m columns which will hold candidate notes for each character. A pseudorandom generator function is used to generate the key matrix. The pseudo random generator function uses a seed value to permute the note set to generate the key matrix. The same seed value will be used on both encryption and decryption side to generate the key matrix.

Table 3. Candidate Notes Along With Channel for Each Character

Character	**Candidate Notes (MIDI Note No, Channel No.)**						
	1	2	3	4	5	6	7
….	….	…..	….	…..	…..	…..	……..
E	54,7	12,6	24,3	18,9	16,7	22,5	22,3

H	111,5	22,4	16,3	12,2	11,7	17,12	27,4
L	11,6	11,2	24,8	17,6	18,3	12,3	11,1
......	.....	.....	......	......	.....	.....	.....
O	65,13	13,7	7,13	22,6	17,9	2,8	18,6
......	....	......	.....	......	....	....	......

3. ENCRYPTION AND DECRYPTION ALGORITHMS

3.1 Encryption Algorithm

The encryption algorithm takes key matrix and the plaintext message and produces the sequence of musical notes as a midi file, which can be transmitted securely over the wired network (refer Figure 7). The key matrix is generated using a seed value which initializes the random function for the random permutation of notes for each character (A part of key matrix is depicted by Table 3). The steps involved in the encryption process are:

- Generate the key matrix.
- Find candidate notes for each character of message
- . Feed candidate notes to the melodic composer.
- Apply fuzzy rules for the music composition and select the best plausible musicalsequence generated.
- Generate the midi file as the encrypted message.

The melodic composer tries various permutations and combination and selects the best combination of notes where notes come sequentially one after another from one of the candidate notes for each character. The selection of the notes depends on the transition probabilities of the notes and fuzzy rules.

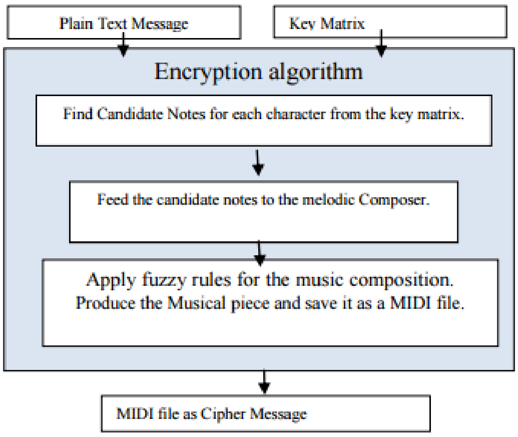

Plain Text Message
Key Matrix
Encryption algorithm
Find Candidate Notes for each character from the key matrix.
Feed the candidate notes to the melodic Composer.
Apply fuzzy rules for the music composition.
Produce the Musical piece and save it as a MIDI file.
MIDI file as Cipher Message

Figure 7. Encryption Algorithm

3.2 Decryption Algorithm

The decryption of the musical notes as a cipher message is simply done by mapping the characters for each note from the key matrix (refer Figure 8). The steps involved in decryption process are:

- Generate the key matrix using the seed value.
- Find the plain text character for each musical note by mapping notes to Character form the key matrix sequentially.
- Save the plain text sequence.

The same seed value is used for generating the exactly same key matrix used on the encryption side.

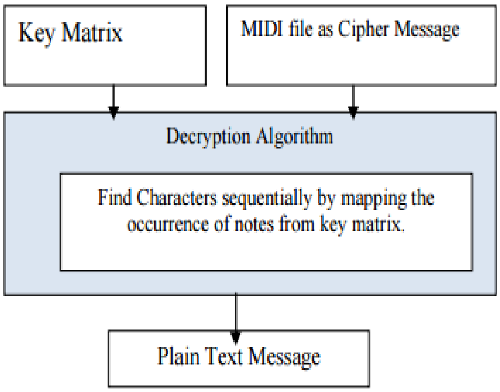

Key Matrix
MIDI file as Cipher Message
Decryption Algorithm
Find Characters sequentially by mapping the occurrence of notes from key matrix.
Plain Text Message

Figure 8. Decryption Algorithm

4. IMPLEMENTATION, RESULT AND DISCUSSION

The proposed algorithm was implemented in MATLAB® . MIDI library functions were used for representation of musical notes. Fuzzy genesis rules were defined depending on the genre used for composition. A pseudo random generator function was used to generate the key matrix. Depending on the characters of the plain text message the candidate notes were fed to the composer. The results of the encryption process were found to be quite satisfactory in terms of aesthetic appeal. The encrypted message in the form of musical piece was found to be more realistic so even after intercepting the communication, the intruder cannot guess the musical piece as a cipher message. The same characters were encrypted into different musical notes depending on the occurrence of the characters in the plain text because of the fact that same character could have been encrypted using one of the several candidate notes. The same text encrypted with the same key produced different musical patterns which was an added feature of the proposed algorithm. The key used in the encryption and decryption is not a simple one-to-one substitution so guessing the key is very hard in practice. The primary goal of enciphering plain text message using musical notes was achieved along with satisfying the second goal as an aesthetic appeal. Complex rules for note density, note duration, note intensity, rhythm and harmony are subject to a specific composition style, which can be adopted by following the styles of well-known composers. These rules then can easily be quantified using fuzzy rules and can be used to encipher messages. Musical cryptography can be seen as a counterpart for audio steganography.

5. REFERENCES

[1] D. Kahn, “The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet”, (1996). J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] D. Davies, “A brief history of cryptography”, Information Security Technical Report, vol. 2, no. 2, (1997), pp. 14-17. K. Elissa, “Title of paper if known,” unpublished.

[3] E. Sams, “Musical cryptography”, CRYPTOLOGIA, vol. 3, no. 4, (1979), pp. 193-201.

[4] E. Sams, “Elgar's Cipher Letter to Dorabella”, The Musical Times, vol. 111, no. 1524, (1970), pp. 151-154.

[5] J. L. Klüber, “Kryptographik”, (1809).

[6] A. Kircher, “Musurgia universalis”, 1650, (1988).

[7] A. P. Coudert, R. H. Popkin, and G. M. Weiner, “eds. Leibniz, mysticism and religion”, International Archives of the History of Ideas, vol. 158, Springer, (1998).

[8] J. Bourne, “The concise Oxford dictionary of music”, OUP Oxford, (2004).

[9] R. Tatlow, “Bach and the Riddle of the Number Alphabet”, Cambridge University Press, (1991).

[10] S. E. Sadie, “The new Grove dictionary of music and musicians”, (1980).

[11] A. P. Coudert, R. H. Popkin, and G. M. Weiner, “eds. Leibniz, mysticism and religion”, International Archives of the History of Ideas, vol. 158, Springer, (1998).

[12] A. Shenton, “Olivier Messiaen's system of signs: notes towards understanding his music”, Ashgate Publishing, Ltd., (2008).