International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Music Cryptography based on Carnatic Music

Deepthi Rao, Shashidhar Koolagudi

Abstract: Music and cryptography have been linked to one another since ancient times. The idea of replacing plaintext letters with music notes and sending the music file to receiver, is not new. But such replacements sometimes result in music clips which are not pleasant to listeners and thereby leading to the music clip gaining unnecessary extra attention. Most of the works done in this area, fail to ensure the generation of a music clip that invariably conforms to any particular form of music. Melody of the music clip is neglected. In order to address this issue, current paper proposes a novel approach for sharing a secret message based on concepts of Carnatic Classical Music. The method proposed here aims at converting a message in textual format to a music clip before sending it to the receiver. Receiver can then decrypt that message using the knowledge of range of frequency values associated with each musical note also called as 'swara' in Carnatic Classical Music. Each plaintext character from English alphabet is replaced by different combinations of swaras. The set of swaras mapped to each plaintext character is so chosen that the final music file produced as the output of encryption always conforms to a melodic form ('Raga') governed by the framework of Carnatic Classical Music. Ten subject matter experts in the field of Carnatic music have given their opinion about the conformance of these music clips to specified ragas. Also, Mean Opinion Score (MOS) of 25 listeners has been tabulated to test and verify the melodic aspect of these music clips.

Keywords : Musical Cryptography, Carnatic Music, Swara, Raga, Encryption, Decryption, Melody, Frequency Analysis, Indian Music, Symmetric Key, Mean Opinion Score.

I. INTRODUCTION

Cryptography- ‘secret writing’ is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the plaintext and the disguised message is called the ciphertext [8]. The idea of maintaining secrecy and concealing messages have gained importance right from the beginning of civilization[3]. As and when a particular method of encryption becomes popular, the danger of cryptanalysis increases and hence new techniques need to be invented or identified to serve the purpose. Musical symbols and musical notes have been used as codes and ciphers from early days. The art of encrypting messages using music is termed as music cryptography [13]. Musical notation is the representation of sound with symbols. Any music can be represented using these symbols [17]. The idea of replacing plaintext characters with musical notes may involve musical notes in the form of visual sequence(musical symbols/notations), vocal or instrumental music.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author
Deepthi Rao*, M Tech. in Computer Science - Information Security National Institute of Technology Karnataka, Surathkal, India - 575025.
Shashidhar Koolagudi, Assistant Professor, Department of Computer Science and Engineering,National Institute of Technology Karnataka, Surathkal, India - 575025.

The current paper is mainly concerned with plain text characters encrypted as sequence of musical notes from an instrument. Encryption in modern era consists of making use of a ‘key’ to convert a meaningful message into some “gibberish” text and similarly get back the message from its encrypted format. In the context of music cryptography, key is a mapping between the plain text characters and musical notes. Symmetric key algorithms use the same key for encryption and decryption. Asymmetric key algorithms are those which use different keys for encrypting and decrypting purpose[4].

The challenging part in designing a music cryptographic scheme is to come up with an appropriate mapping of plain text characters to musical notes so that the final musical sequence generated is a valid one. Validity of a musical sequence is decided based on how pleasant and melodic it sounds, to a listener. Various methods have been proposed earlier which merely describe novel mapping schemes without paying much heed to the melody aspect. As a result, messages encrypted using such approaches may unnecessarily draw the attention of an adversary. Requirement for a scheme that can produce a musical composition which is both natural as well as pleasant was necessitated by these outcomes. The proposed approach is built on the foundations of Carnatic music wherein the textual characters are replaced with musical notes and the music clip so generated invariably conforms to the framework of Carnatic music, thus taking care of the melody aspect/pleasantness of the music clip. The remainder of this paper is organized as follows. Section II gives a brief overview of a few works done in the area of music cryptography. It is followed by Section III which is dedicated for a small introduction about Carnatic Classical Music. Section IV includes all the details about the proposed approach. Section V contains a discussion on results and highlights of proposed method. Section VI concludes the paper and sheds some light about the possible future work.

II. LITERATURE SURVEY

Music is considered to be a mode of communication well understood and appreciated by a majority. History says that many of the cryptologists have been good musicians. Also, notable composers like Schumann, Michael Haydn, Elgar and Tartini were known to be interested in cryptography. In fact, the fields of music and cryptography have positive correlation. The connection was also known to and used by the British wartime crypto-analytic service [19]. Earliest forms of music cryptography made use of the simple method of replacing characters of the plaintext with musical symbols. Edward Elgar, a notable composer wrote a letter to Miss Dora Penny in encrypted form which is famous as ‘Dorabella Cipher’ [6]. Bach, another musician regularly employed the natural order number alphabet (A=1 to Z=24) in his work.

Using this, he is said to have incorporated significant words into his music and provided himself with a symbolic composition scheme [22].

Considerable amount of work has been done in the field of music cryptography in recent years too. [4] proposed a scheme to encrypt plaintext characters comprising of English letters as well as digits 0-9 by randomly assigning each plaintext character to a number between 12 and 23, which in turn represent 36 different music notes.[5] described a method that took 12 notes and 6 octaves, generating 72 music notes which can be used to replace plaintext characters. This method made use of a transition table and note transition algorithm in order to specify the mapping of plaintext characters to music notes. A method to encrypt binary strings using concepts of graph theory and propagating cipher block chaining (PCBC) mode of encryption was discussed by [23]. Each string of three bits was mapped to a music note. One such 3-bit combinations corresponds to a pause/blank in the music clip. In [16], a method that used the concepts of magic-square and Polybius cipher techniques was explained. A 6X6 magic square was selected and all English letters and 0-9 digits were placed in each of its cells. Each column and each row of this magic square was labelled with C,D,E,F,G,A. Each plaintext character was thus replaced by its corresponding row-column index in the magic square. Space character was replaced by the music note B. Two more methods to encrypt binary strings were discussed in [24]. Both these methods considered two binary strings (one of which was the plaintext string to be encrypted) and inserted one of them into the other at specific locations in order to generate a third string. Groups of bits in that final string were mapped to different music notes. [11] proposed a method of music cryptography that made use of genesis rules and the concept of raga in Indian classical music. It was based on replacing each plaintext character with a swara from a specified raga depending on the probability of its occurrence in that raga. A method making use of a fuzzy logic was explained in [13]. This made use of various constraints like melodic rules, harmonic rules, rhythm rule, etc in order to generate multiple music clips corresponding to a text message. After that, fuzzy rules were applied and the music clip with best possible musical sequence was selected and converted to a MIDI file before sending to the receiver. In [12], a combination of Playfair cipher and Polybius cipher techniques was used for encryption. Initially plaintext was encrypted using Playfair cipher. The encrypted message was re-encrypted using Polybius cipher. A permutation algorithm was used to generate the key matrix which was used to map the text characters to corresponding music notes.[14] proposed an encryption scheme that generated a cipher key which abided by the conventions of music theory. Dissonance and uneven beats were avoided by creating a key that stayed in one key signature in the context of a single major scale.

III. INTRODUCTION TO CARNATIC MUSIC

Indian classical music can be broadly classified into two categories– Hindustani classical music and Carnatic classical music. While the former is popular in north India, the latter form is widely practiced in the southern parts of India. ‘Raga’ and ‘Tala’ are considered to be the crux of music. Raga and tala can be thought of as equivalent to melody and rhythm in western music [21]. Individual mu-sic notes that form a composition are called as ‘swara’s. ‘Sa’, ‘Ri’, ‘Ga’, ‘Ma’, ‘Pa’, ‘Dha’ and ‘Ni’ together called as ‘saptha swaras’, form the basis of Carnatic Classical Music. These saptha swaras can be considered similar to the western musical notes C,D,E,F,G,A,B. We know that each of these seven music notes in western music has its variants like C#,D#,E# and so on. Similarly in saptha swaras, except for]Sa’ and ‘Pa’ , every other swara has its own variant. For example, ‘Ri’ has ‘Ri1’, ‘Ri2’ and ‘Ri3’ as its variants where each of them has its own pitch. Sa and Pa are termed as ‘shuddha swaras’ or pure notes as they do not have a variant. Each of these seven swaras can be associated with certain frequency values. TABLE I which was created based on A440 pitch standard shows the swara-frequency mapping along with the name of corresponding in western musical note. A440 is the standard pitch adopted by the United States Government in 1920[7].

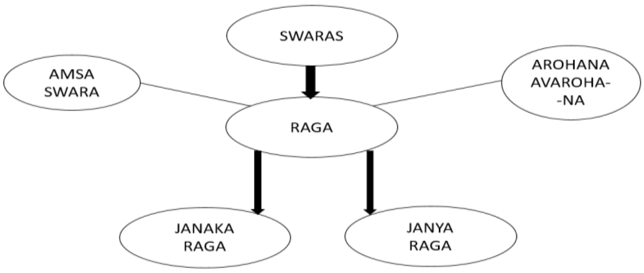

Fig. 1.Representation of the connection between Swaras, Ragas and their types

A. Raga

A ‘raga’ in Carnatic Music is a melodic form governed by certain rules. Although raga can be thought of as equivalent to melody in Western music, it is much more complex than just that [21]. A raga can be classified as either a ‘Janaka Raga’ (also known as ‘Melakarta Raga’) or a ‘Janya Raga’. A melakarta raga will have all the seven swaras and a janya raga will have at least 5 of the seven swaras. There are 72 Janaka ragas [10].

It is to be noted that, only one variant of a swara can appear in a raga. For example, all three variants of Ri - Ri1, Ri2, Ri3 can never occur in any one raga. Similarly other swaras and their variants.

A raga is defined by its fixed set of swaras. The ragas differ from one another based on the combination of swaras and their variants (if any) which are considered to be valid in them.

Each raga is characterised by its ‘arohana’ and ‘avarohana’. Arohana is the sequence of swaras used in a raga in the ascending passages i.e. as the pitch goes up.

Avarohana is the sequence of swaras to be used in descent. Looking at the arohana and avarohana of a raga, one can know which swaras (swara-variants) are valid in that raga.The arohana and avarohana of a raga provide only emaciated outline upon which the rest of the raga is formed [20].

B. Amsa Swara

Just like various checkers in the game of chess, swaras in a raga have different functions. Some swaras are considered to be more important than the rest [9].

In the context of a raga, ‘chayya swara’ is a note that brings out the characteristic - melodic entity of the raga and ‘dhirga swara’ is that which can be played as a long note.

Certain swaras of a raga are called as ‘amsa swara’s of that raga. Each raga will have unique amsa swara(s). Amsa is a swara that describes the melodic entity in the raga and hence considered the soul of that raga. It is also a chayya swara and a dhirga swara [18].

Thus significance of amsa swara is that, it can add to the beauty of a musical composition by being played repeatedly and/or as a long swara, making the resulting music pleasant to listeners.

Figure 1 represents some of the concepts of Carnatic Music explained earlier. It shows that swaras combine to form different ragas, ragas are classified as janaka and janya ragas and certain features of a raga such as amsa swara and arohana-avarohana.

TABLE I: Swara-Frequency Mapping (A440 pitch standard)

swara	Frequency (Hz)	Note
Sa	260.29	C
Ri1	277.84	C#
Ri2 , Ga1	293.08	D
Ri3 , Ga2	309.66	D#
Ga3	330.28	E
Ma1	346.90	F
Ma2	372.19	F#
Pa	390.61	G
Dha1	414.82	G#
Dha2 , Ni1	440.00	A
Dha3 , Ni2	462.33	A#
Ni3	495.84	B

IV. PROPOSED APPROACH

This method considers a plaintext alphabet that consists of the 26 letters of English along with space character resulting in a set of 27 characters. The proposed approach makes use of only janaka ragas. Depending on the selected raga, all of its swaras except for an amsa swara, are assigned with position weights. Each of these six positions can take a weight of 0 or 1, resulting in 64 possible combinations. Each of these six bit combinations can be used to represent one plaintext character. 1 in the position of a swara indicates that it is considered for encrypting that plaintext character while 0 indicates that it is not.

Combination with all 0’s indicates the absence of all six notes. This corresponds to a ‘pause’ in the music sequence. Depending on the plaintext character that is mapped to this 000000/pause, final music sequence may contain multiple pauses. This is unnatural and hence makes the music clip vulnerable to attack. Considering this, 000000 is not used for encryption in this scheme.

Combinations with a single 1 in any position imply that a single swara is used to represent a plaintext character. This leads to a one-to-one mapping between musical notes and plaintext letters thereby making it prone to frequency analysis attack. Thus all the combinations with a single 1 are also discarded.

Mapping a single plaintext character to a sequence with more than three swaras is not advised as they result in a very lengthy cipher text compared to the plaintext. This might cause some processing overhead. Thus such combinations are also not considered for our purpose.

Considering the combinations with 1s in two places, results in just 15 options while there are 26 letters in English alphabet. Thus 11 combinations with 1 in three places are also considered. To optimize this mapping of a plaintext letter to a ‘swara-sequence’ , more frequently occurring letters in English are mapped to sequences of 2 swaras while less frequently occurring letters are assigned sequences of 3 swaras. This considerably reduces the possible overhead. While assigning position weights, an amsa swara (say, ‘x’) was left out. It is considered now. A demarcation between adjacent plaintext letters is indicated by playing amsa swara once (‘x’) and the space character is indicated by playing it twice (‘xx’).

The plaintext alphabet to swara sequence mapping is considered as the symmetric key in this method. As mentioned in [18], to use a private-key scheme like this, the legitimate parties should initially agree on the secret key which is done by having one party generate the key at random and sending it to the other party using a secure channel. The key is generated independently of the plaintext.

Swara variants used in the music sequence vary depending on the selected raga. Also, mapping with respect to the selected raga need not be unique. That means, it is up to the sender and receiver to decide: (a) which eleven combinations of three 1’s they select (b) which amsa swara is selected (c) which swara sequence should be mapped to which plaintext letter. Thus multiple mappings are possible for a given raga.

A. Illustration

One of the popular ragas called ‘Mayamalavagowla’ is considered here to demonstrate the proposed approach. Its arohana is: Sa Ri1 Ga3 Ma1 Pa Dha1 Ni3 Sa. An amsa swara of this raga is ‘Pa’. Hence except for it, assign position weights to other six swaras - ‘Sa’, ‘Ri’, ‘Ga’, ‘Ma’, ‘Dha’, ‘Ni’. Once all combinations with two 1’s are used, randomly select combinations with three 1’s to encrypt the remaining plaintext letters.

‘Pa’ is used as a letter demarcation and ‘PaPa’ corresponds to a space character in plaintext. Now, ‘Pa’ is naturally the most occurring swara in the musical sequence generated. Since ‘Pa’ is an amsa swara of this raga, this repetition makes the music clip natural and pleasant.

It is to be noted that TABLE II shows one possible plaintext-ciphertext mapping for raga Mayamalavagowla.

TABLE II: Plaintext Alphabet-Swara Sequence Mapping for Raga Mayamalavagowla

Alphabet	Swara Sequence
A	Ma Dha
B	Ri Dha Ni
C	Sa Ma
D	Ri Ga
E	Dha Ni
F	Sa Ri
G	Ga Ma Ni
H	Ri Dha
I	Ga Ni
J	Ri Ga Dha
K	Ri Ma Dha
L	Sa Ni
M	Sa Ga
N	Ga Dha
O	Ga Ma
P	Ga Ma Dha
Q	Ri Ga Ni
R	Ri Ma
S	Ri Ni
T	Ma Ni
U	Sa Dha
V	Ri Ma Ni
W	Ma Dha Ni
X	Ri Ga Ma
Y	Ga Dha Ni
Z	Sa Ma Ni
Space	Pa
Letter Demarcation	PaPa

Raga ‘Shankarabharana’ with arohana Sa Ri2 Ga3 Ma1 Pa Dha2 Ni3 Sa, raga ’Kharaharapriya’ with Ri2 Ga1 Ma1 Pa Dha2 Ni1 Sa as arohana and raga ‘Kalyani’ with arohana Sa and Sa Ri2 Ga3 Ma2 Pa Dha2 Ni3 Sa, also have ‘Pa’ as their amsa swara. Thus, the mapping shown with respect to Mayamalavagowla is applicable to these ragas as well. Note that since no two variants of the same swara can occur in a raga, Ri1 in Mayamalavagowla and Ri2 Shankarabharana have been represented by just Ri. Similarly for other swara variants too.

For clarity, a mapping with respect to raga ‘Harikambhoji’ having arohana- S R2 G2 M1 P D2 N1 S and amsa swara ‘Ma’ is shown in TABLE III.

TABLE III: Plaintext Alphabet-Swara Sequence Mapping for Raga Harikambhoji

Alphabet	Swara Sequence
A	Pa Dha
B	Ri Dha Ni
C	Sa Pa
D	Ri Ga
E	Dha Ni
F	Sa Ri
G	Ga Pa Ni
H	Ri Dha
I	Ga Ni
J	Ri Ga Dha
K	Ri Pa Dha
L	Sa Ni
M	Sa Ga
N	Ga Dha
O	Ga Pa
P	Ga Pa Dha
Q	Ri Ga Ni
R	Ri Pa
S	Ri Ni
T	Pa Ni
U	Sa Dha
V	Ri Pa Ni
W	Pa Dha Ni
X	Ri Ga Pa
Y	Ga Dha Ni
Z	Sa Pa Ni
Space	Ma
Letter Demarcation	MaMa

B. Encryption

Consider the plaintext message- ‘Knowledge is power’ and raga used is ‘Mayamalavagowla’. Plaintext character ‘K’ is replaced by ‘RiMaDha’ in cipher text, ‘Pa’ is used to indicate the end of one letter; ‘n’ is replaced by ‘GaDha’, followed by ‘Pa’; ‘o’ corresponds to ‘GaMa’ followed by ‘Pa’; ‘w’ corresponds to ‘MaDhaNi’ followed by ‘Pa’ and so on till the end of the word ‘Knowledge’. Swara sequence ‘PaPa’ is used to indicate the end of a word. Same process continues till the end of the plain text. Swara sequence obtained after each plaintext character replacement is :

RiMaDhaPa GaDhaPa GaMaPa MaDhaNiPa SaNiPa DhaNiPa RiGaPa GaMaNiPa DhaNiPaPa GaNiPa RiNiPaPa GaMaDhaPa GaMaPa Ma DhaNiPa DhaNiPa RiMaPaPa

TABLE I is used to note frequency value corresponding to each swara in the above sequence. Sine wave for each of these frequencies is generated and concatenated in the end to produce a single music clip for the given plaintext. This music clip is then sent to the receiver. Figure 2 depicts the process of encryption.

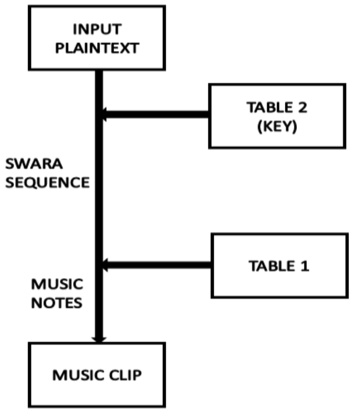

Fig. 2. Process of Encryption

C. Decryption

Input for deciphering algorithm is the music clip received from the sender. Knowing the sampling frequency of this music clip, it can be split into its component samples. Peak frequency value of each sample is noted and approximated to a swara using TABLE I.

From the sequence of swaras , corresponding plaintext message can be obtained by making use of TABLE II. Figure 3 depicts the process of decryption.

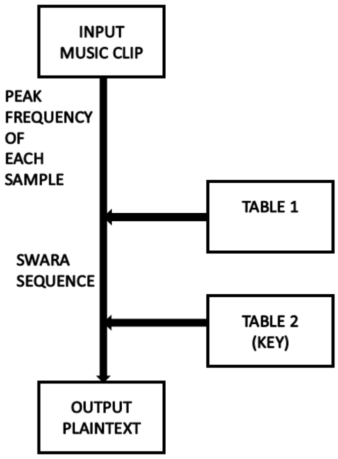

Fig. 3. Process of Decryption

D. Summary of the Proposed Scheme

Steps of the proposed method can be put as follows:

- Sender and receiver agree upon a raga and key. TABLE II is a sample key.
- For encryption, replace each plaintext letter with its corresponding swara sequence. Refer TABLE II.
- From the swara sequence obtained in previous step, generate a music clip having frequency values corresponding to each swara. Refer TABLE I.
- Sender sends the music clip to the receiver.

V. DISCUSSION

The proposed method has been implemented and verified for plaintext files chosen from RFC dataset. While creating a music file corresponding to the given plaintext message, playing each musical note for longer duration will increase the size of encryption output. At the same time, playing each note for a very short time will make the resulting musical composition unpleasant and unnatural. Hence, as a tradeoff between quality and size, a duration of 0.20s for each note is chosen during implementation. Figure 4 shows the details of time needed to encrypt text files of different lengths. Figure 5 shows the time required for decryption Vs the size of input text file size. Figure 6 denotes the size of music files generated for different lengths of text files. All three figures 4, 5 and 6 were generated with the help of MATLAB functions.

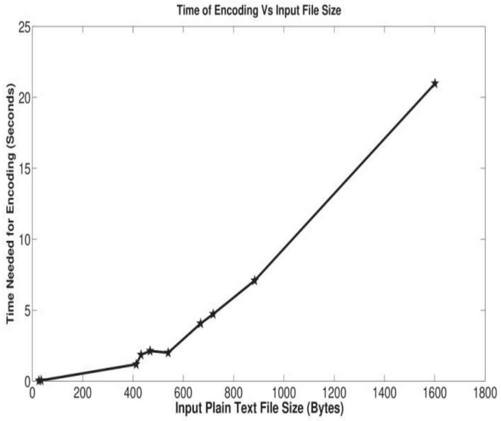

Fig. 4.Encryption Time Vs Input Plaintext Size

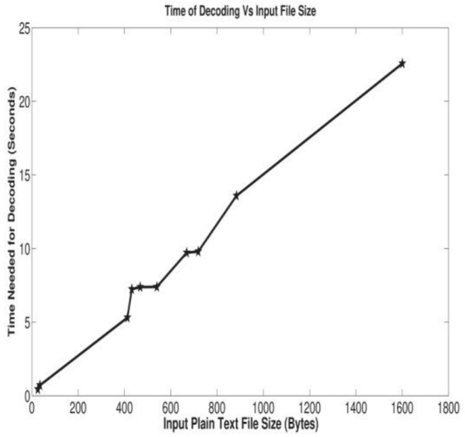

Fig. 5.Decryption Time Vs Input Plaintext Size

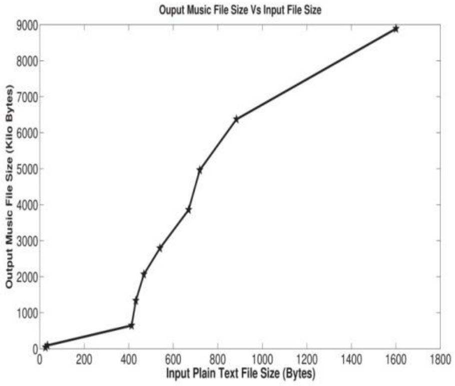

Fig. 6.Output Music File Size Vs Input Plaintext Size

Highlights of the proposed approach :

- The method makes use of Carnatic Classical Music concepts like raga, swara-frequency relationship, amsa swara, etc and produces a valid, pleasant musical note sequence. This provides least scope for an attacker to make a guess that the music clip is a secret message and not just a sequence of musical notes. The conformance of such a music clip to a specific raga has been verified and confirmed by a few musicians.

- A survey was conducted using the plaintext message 'Knowledge is Power'. Five different ragas such as Mayamalavagowla, Kharaharapriya, Harikambhoji, Kalyani and Shankarabharana were used for encrypting it. These five clips and a list of the above mentioned ragas were sent to ten musicians well aware of Carnatic classical music. Participants of the survey were asked to match each music clip to its raga from the given list. Opinion of each participant was logged. Based on this, a pie chart for each raga was drawn to depict what percentage of these musicians agree with expected raga.

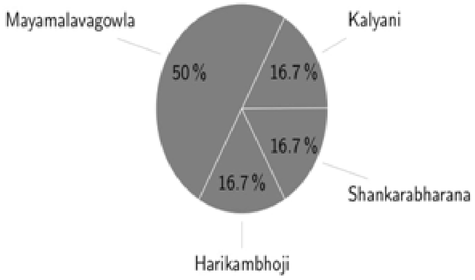

Fig. 7.Survey result of music clip generated for message encrypted using raga 'Mayamalavagowla'

Pie charts shown in figure 7 and figure 8 depict the survey results for the clips created using ragas Mayamalavagowla and Kharaharapriya respectively. We can see that 50 percent of the people agree with the expected raga Mayamalavagowla and 66.7 percent of the people agree with conformance to Kharaharapriya .

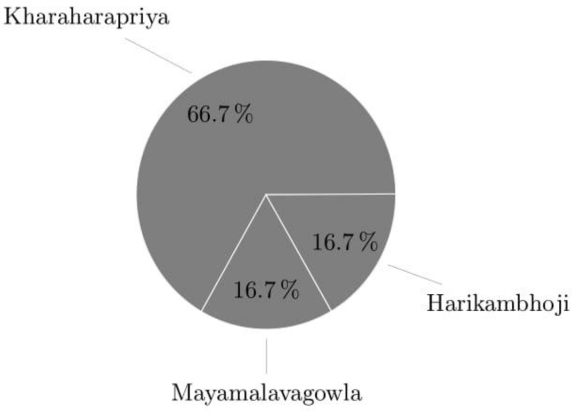

Fig. 8.Survey result of music clip generated for message encrypted using raga 'Kharaharapriya'

- The method ensures that shorter swara sequences are assigned to more frequently occurring plaintext characters and longer sequences are assigned to less frequently occurring ones. This considerably reduces the possible size overhead.
- Cryptography aims at converting a secret message into an unintelligible text while steganography aims at hiding the secret message inside a cover medium which could be an audio/text file. The proposed method is concerned with converting a secret text message into an audio clip which is itself the secret being sent and hence is somewhat linked to both the concepts of cryptography and steganography.
- There is no one-to-one mapping of a single alphabetical character to a swara/musical note in the proposed method. The frequency analysis based attack which is possible in most of the existing approaches can be avoided here.
- As explained earlier, multiple mappings are possible for a given raga. Even if an attacker with some knowledge of Carnatic music is able to identify the raga from a music clip, he/she will not be able to decrypt it without knowing the swara-sequence to plaintext mapping(key). Thus ciphertext-only and man-in-the-middle attacks can be avoided.
- Three methods have been compared and ranked based on Mean Opinion Score (MOS). [2] has details on MOS calculation. MOS was calculated as follows. 'Knowledge is Power' was chosen as the plaintext. It was encrypted using existing method [15], existing method[24] and proposed method using five different ragas. Resulting music clips were indexed by numbers 1-7. For our calculations, 25 listeners were asked to provide a rating (in the range 1-5) for each music clip depending on how

TABLE IV: Calculation of MOS as per Opinions of 25 People for 7 Music Clips Created Using 3 Methods : Method 1 is explained in [15], Method 2 is discussed in [24] and Method 3 is the proposed method

Index (i)	Method Used	Raga	Excellent (5)	Good (4)	Fair (3)	Poor (2)	Bad (1)	(w_i)	(M_i)
1	Method 1	Not Applicable	-	-	11	12	2	59	2.36
2	Method 2	Not Applicable	8	11	6	-	-	102	4.08

3	Method 3	Kalyani	11	13	1	-	-	110	4.4
4	Method 3	Mayamalavagowla	2	12	9	2	-	89	3.56
5	Method 3	Harikambhoji	12	11	2	-	-	110	4.4
6	Method 3	Shankarabharana	2	12	10	1	-	90	3.6
7	Method 3	Kharaharapriya	2	8	13	2	-	85	3.4
Sum	-	-	37	67	52	17	2	645	3.68

pleasant it sounded to them where 1 indicates low pleasantness and 5 indicates high pleasantness. TABLE IV was formed during the MOS calculation. Columns 4-8 show how many people among 25, have given the rating specified in the respective column headers, for each music clip. Weighted score and MOS are given by the expressions (1) and (2) respectively. In the last row of TABLE IV, columns 4-9 show the sum of each column. The value 3.68 in tenth column of last row corresponds to system average i.e. the overall mean calculated by using expression (3). We can observe that the MOS of music clip created using [15] is 2.36 which is way below system average. Music clip created using [24] has MOS of 4.08 which is higher than system average. By taking average of 5 MOS values for the music clips created using proposed method, we get a value of 3.872 [i.e. (4.4 + 3.56 + 4.4 + 3.6 + 3.4) / 5] which is greater than the overall mean. MOS values for each music clip generated using proposed method are either above system average or close to it. It has to be noted that, in method [24] if the random fake string generated results in the creation of a musical clip with multiple pauses, the pleasantness of the music clip will naturally reduce.

$$\boldsymbol{w_i} = 5*E + 4*G + 3*F + 2*P + 1*B \qquad (1)$$

where,

$\boldsymbol{w_i}$- is the weighted score of the music clip indexed $\boldsymbol{i}$

E- is the number of people who rated music clip $\boldsymbol{i}$ with a score 5

G - is the number of people who rated music clip $\boldsymbol{i}$ with a score 4

F - is the number of people who rated music clip $\boldsymbol{i}$ with a score 3

P - is the number of people who rated music clip $\boldsymbol{i}$ with a score 2

B - is the number of people who rated music clip $\boldsymbol{i}$ with a score 1

$$M_i = w_i / N \qquad (2)$$

where,

M_i -is the MOS of the music clip indexed $\boldsymbol{i}$

w_i -is the weighted score of music clip $\boldsymbol{i}$

N -is the total number of people considered while calculating the w_i (in this example, N = 25)

The MOS values give an overall picture about the pleasantness of the music clips generated using each of the three methods.

$$Avg = 1 / (n * N) \sum_{i=1}^{n} w_i \qquad (3)$$

where,

Avg - is the system average/overall mean

wi - is the weighted score of music clip i

n - is the number of music clips considered (in this example, n = 7)

N - is the total number of people considered while calculating the wi (in this example, N = 25)

VI. CONCLUSION AND FUTURE WORK

The proposed method is a new and creative approach of secret sharing. It is found to be better than some of the existing approaches like [24] and [15] in terms of size and pleasantness of music clip. Since this method stresses upon abiding by the rules of Carnatic classical music, the resulting music clip invariably conforms to a raga and hence gains very less unnecessary suspicion from an attacker. Future work can be done by including the following point for improvement. There is a concept of 'gamaka' in Carnatic Classical Music. A 'gamaka' is considered to be an ornamentation to a musical composition. Gamakas are basically connective forces from one swara to another. They can as well be defined as the manner of travel from one swara position to another [1]. Every raga has its own rules with respect to inclusion of gamakas. The concept of gamaka can be incorporated to add richness to the musical sequence generated during encryption according to Sangeeta Shastra conventions.

ACKNOWLEDGMENT

First Author thanks the support, encouragement and guidance received from Sri CN Shankar Rao and Dr. Saraswathi Rao throughout the process of implementation and publication of the proposed method.

REFERENCES

1. Arun and Choodamani Nandagopal. “Alamkara - Gamaka: An Anthology”. In: IOSR Journal Of Humanities And Social Science (IOSR-JHSS) 20 (2015).
2. Milos Cernak and Milan Rusko. “An evaluation of synthetic speech using the PESQ measure”. In: Proc. European Congress on Acoustics. 2005, pp. 2725–2728.

3. Tony. M. Damico. A Brief History of Cryptography. 2009.
4. Sandip Dutta, Soubhik Chakraborty, and NC Mahanti. “A Novel Method of Hiding Message Using Musical Notes”. In: International Journal of Computer Application 1.16 (2010).
5. Sandip Dutta, Chandan Kumar, and Soubhik Chakraborty. “A symmetric key algorithm for cryptography using music”. In: International Journal of Engineering and Technology 5.3 (2013), pp. 3109–3115.
6. Elgar Eric Sams. “Elgar’s Cipher Letter to Dorabella”. In: The Musical Times 111.1524 (1970), pp. 151–154.
7. Ross King. Recorded music pitch and tempo adjustment indicating device. US Patent 2,142,591. Jan. 1939.
8. Neal Koblitz. A Course in Number Theory and Cryptography. 2nd ed. Springer-Verlag New York, 1994.
9. Gopala Krishna Koduri et al. “Raga recognition based on pitch distribution methods”. In: Journal of New Music Research 41.4 (2012), pp. 337–350.
10. Professor Venkatarama Krishnan. “Mathematics of Melakartha Ragas in Carnatic Music”. In: UMass Lowell (2012), pp. 2–3.
11. Chandan Kumar, Sandip Dutta, and Soubhik Chakraborty. “Musical cryptography using genetic algorithm”. In: Circuit, Power and Computing Technologies (ICCPCT), 2014 International Conference on. IEEE. 2014, pp. 1742–1747.
12. Chandan Kumar, Sandip Dutta, and Soubhik Chakraborty. “A Hybrid Polybius-Playfair Music Cipher”. In: International Journal of Multimedia and Ubiquitous Engineering 10.8 (2015), pp. 187–198.
13. Chandan Kumar, Sandip Dutta, and Soubhik Chakraborty. “Hiding Messages using Musical Notes: A Fuzzy Logic Approach”. In: International Journal of Security and Its Applications 9.1 (2015), pp. 237–248.
14. Norissa Lamaute et al. “A Substitution Cipher for Musical Cryptography”. In: (2016).
15. Shant Mahserejian. Music encryption. http://math.ucsd.edu/˜crypto/ Projects / ShantMahserejian / Music.pdf. June 2005.
16. Moumita Maity. “A Modified Version of Polybius Cipher Using Magic Square and Western Music Notes”. In: International Journal for Technological Research in Engineering 1.10 (2014).
17. Yamuna Manimuthu. “CRYPTOGRAPHY USING MUSIC NOTES”. In: Journal of Global Research in Computer Science 4.4 (2013), pp. 100–102.
18. Ashish Pandey. Encyclopaedic Dictionary of Music. Isha Books, 2005.
19. Eric Sams. “Musical Cryptography”. In: Cryptologia 3.4 (1979).
20. Surendra Shetty and KK Achary. “Raga mining of Indian music by extracting arohana-avarohana pattern”. In: International Journal of Recent Trends in Engineering 1.1 (2009), pp. 362–366.
21. Rajeswari Sridhar and TV Geetha. “Raga identification of carnatic music for music information retrieval”. In: International Journal of recent trends in Engineering 1.1 (2009), pp. 1–4.
22. Ruth Tatlow. Bach and the Riddle of the Number Alphabet. Cambridge University Press (21 February 1991), Apr. 2006.
23. M Yamuna et al. “Encryption of a Binary String using music notes and graph theory”. In: International Journal of Engineering and Technology 5.3 (2013), pp. 2920–2925.
24. M Yamuna et al. “Insertion Method Using Music Notes”. In: Innovare Journal of Engineering and Technology 2.3 (2014).

AUTHORS PROFILE

Deepthi Rao,M.Tech. in Computer Science - Information Security

National Institute of Technology Karnataka, Surathkal, India - 575025.

Shashidhar Koolagudi Assistant Professor, Department of Computer Science and Engineering, National Institute of Technology Karnataka,Surathkal, India - 575025.