Encrypting Messages Using Musical Notes By Genetic Algorithm

[1]Shraddhali N. Patil, [2]Dhanashree H. Parab, [3]Akshay Nambly, [4]Linda Mary John,

[1,2,3,4]Department of Computer Science, St. John College of Engineering and Management, Mumbai, Maharashtra, India.

[1]shraddhali1702@gmail.com, [2]dhanashreeparab2112@gmail.com, [3]nambly77@gmail.com, [4]lindamaryj70@gmail.com

Abstract Cryptography consists of two parts , Encryption and Decryption. When the message is sent to the receiver using cryptography, it is changed which means it is encrypted before it is sent. The encryption makes the message unreadable or recognizable so that no intruder can find the secret in it. The changed text is called as the cipher text. Someone who wants to read it should decrypt it back to the original message. The process of getting back the hidden message from the cipher text is called as the decryption. Cryptography is the combination of both encryption and decryption of any message, file etc. This is a very vast field in the area of Information Security. The cryptographic algorithms are Asymmetric key cryptography and Symmetric key cryptography. When the same key is used for both encryption and decryption, it is Symmetric Key cryptography and when different keys are used for encryption and decryption, it is known as the Asymmetric key cryptography. In cryptography, a key is a parameter that determines the cipher that is the functional output of the algorithm. Without a key, the algorithm would generate no useful output.

Keywords —Asymmetric key, Crossover, Cryptography, Genetic algorithm, Musical Cryptograms, Mutation , Population, Symmetric key

I. INTRODUCTION

Communication has become a very vital part of the life. So, maintaining security is important in transferring the data from one person to another without getting tampered. One of the ways to secure information is cryptography. Cryptography is the practice and study of hiding information, sometimes called as code, but this is not right. It is the science used to keep information confidential and safe from third parties. The cryptography is mixture of various subjects. Cryptography is used in ATM cards, computer passwords, and shopping on the internet etc for various day to day activities. Musical cryptography is using musical ideas and symbols for communicating by sending the encrypted message as notes. Any musical has the seven basic keys. Our Indian music has seven keys Sa, Re, Ga, Ma, Pa, Dha, Ni and the western notes are based on seven keys C, D, E, F, G, A, B. Using this notes, the music is generated. In the paper, a technique of encrypting the text message using western music notes. The musical cryptogram is the sequence of the notes which can be taken to refer to a text by some logical relationship between the names and letters. The use of music notation to encode messages for reasons of personal security called steganography is much rarer. The Genetic algorithm is the process of natural selection which belongs to the larger class of evolutionary algorithms. It is used to provide high-quality optimization solutions and find problems by using crossover, mutation and selection. It requires a fitness function for evaluating solution domain and the genetic representation of the solution domain . The population contains a number of solutions and its size is depended on the problem nature . The selection is the process in which the portion of the population is used to generate new generation. The individual solutions are selected using fitness based process in which the solution with the higher fitness function is selected. The crossover is an operator used in generating the new chromosomes to next generation. There are different types of the crossover techniques Single-point, Two-point, etc. The mutation is another operator used to manage the diversity from one generation population to the next. Mutation alters one or more gene values in a chromosome from its initial state which may change entirely from the previous solution.

Hence, GA can come to a better solution by using mutation. The different types of mutation are bit string, flip bit, boundary, uniform, non-uniform, shrink etc.

II. LITERATURE REVIEW

A system has been developed using MATLAB 2008R, in which 26 alphabets (a to z) and 0 to 9 numbers has been considered as -12 to 23 as the musical notes. These 36 numbers i.e.10 numbers and 26 alphabets are positioned randomly and then these numbers are assigned musical notes -12 to 23. These notes are divided into three octaves (lower, middle and upper). Certain rules are predefined based on which the numbers are converted to vector. This vector and frequency (sound(y, Fs)) are given as input to the speaker on the system. A stereo sound is played on platforms that support it and a sound card is used. Thus the generated music file is given to the receiver. The receiver decrypts the messages by some predefined rules. It is simple and less complex. It takes very less processing time and storage space. A very large message including, an image can be sent. This algorithm does not require searching of any such key in any such public. This algorithm does not require searching of any such key in any such public domain or any private domain. Use of no keys makes it less secure. Music does not sound natural. Security problems limit its usability.[7]

In this technique, the musical notes are related to each letter in the plaintext. Various combinations of each node is generated in which more than one combination of the Musical notes is used for generation of musical sequence. The entropy of each combination is used to calculate the best out of it then it selects the combination with the highest entropy. The cipher text is represented as sine waves. The final cipher text is obtained by writing these waves into media file using the MATLAB. More Secure compared to normal Propagation Cipher Block Code method. More flexible and less complex in nature. This method can be used only for conversion of Binary String format not other.[5]

An algorithm is used which converts the plaintext into musical piece with replacing the characters of plaintext by generated musical notes respectively. Particular character sequence of the plaintext message has its own sequence of the musical notes which mimics the musical pattern present. The sender sends this musical pattern to receiver as a music file. Encryption/Decryption key has a seed value which is transferred using asymmetric algorithm that is RSA in which the key maps the letters to the corresponding musical notes. An n x n matrix is used as an encryption key. The matrix will be produced with the help of the seed value of the key on both the sides that is sender and reciever. It makes use of Symmetric Key Cryptography which makes it more Secure compared to the previous Approach. The probability of guessing the key is 1/72^72 which makes it nearly impossible to find the key. Used for conversion of text messages only.[2]

A multiple note substitution algorithm is used to overcome the drawbacks of using an only limited number of letters in the plaintext message. The application of the algorithm is to produce a cryptic message that helps in hiding the message in the musical notes and also decreases the chance of being recognized as the cipher. In the encryption, all the possibilities of the musical notes of letter in the plaintext are found with the help of the key matrix. There is a minimum of two possible substitutions for a letter and maximum of three possible substitutions for a letter .Then combinations of each note are obtained. Even though there is more than one combination of musical note for the plaintext, only one combination of the musical note is used for the creation of cipher text. The best combination of musical notes can be obtained by calculating the entropy of each combination and choosing the combination with the highest entropy. The resultant musical piece is hard to crack as the key is like a one time pad. The proposed algorithms do not apply any constraints on the number of the letters in the plaintext message. There are more than one possible substitutions for a letter. As the number of substitutions for the letter increases the space required for storage and the time required for calculations also increases.[1]

A fuzzy logic based algorithm is proposed for musical cryptography. The paper uses a symmetric key substitution on cipher which encrypts a particular character using one of the n candidate notes. Fuzzy logic is being used in Musical cryptography to produce the musical sequence which is hard to detected as the cipher. In encryption, the key matrix and plaintext are taken as input which produces the output a midi file, that can be safely transmitted over wired network. The key matrix is generated using a seed value which initializes the random function for the random permutation of notes for each combination. The results of encryption were quiet satisfying. The same keys are used to encrypt the same text which produces different output. The key is not used as a one to one substitution which makes it difficult to guess. (in a formal manner) Fuzzy logic is completely based on approximations. Fuzzy logic does not have the ability to learn and adapt after solving a problem.[3]

The Genetic algorithm is used for improving the musical composition. Using the initial population generated by the user the program generates composition based on the initial allows the code to take decisions which can be made using musical theory using genetic algorithm. The resultant i.e best composition was then presented to user for evaluation of results. The effectiveness of this method was tested as initial and final was ranked on the scale of 1 to 10. The subjects

expressed an important preferred for the evolved. The composition generated by this method were rated as better as per human ratings. The results proved to be satisfactory for small subject population and not for the large subject population.[6]

Asymmetric key algorithm is based on genetic algorithm is being proposed to check cipher text which is optimal sequence of notes. Hiding the messages in the form of musical patterns not only hides the message as a musical piece but also reduces its chance of being detected as ciphered message. A new technique can be used which converts the messages into musical cryptograms which are nothing but the sequence of musical notes which are soothing to ears. This technique gives satisfactory results when compared to substitution cipher. There is no need to make use of a cover file to hide the message required in steganography. This solves the payload problem usually faced in steganography. The key is one time pad which makes it hard to break. The permutation and combinations used in this technique make it difficult to decrypt the cipher text thus reducing the chance of cipher message being detected as a cipher. An increase in the number of iteration increase its complexity.[4]

III. METHODOLOGY

A. Genetic algorithm

The genetic algorithm is a way of solving both the constrained and unconstrained which are based on the natural selection and is a process that drives biological evolution. The genetic algorithm modifies the individual offspring again and again. At every step, the genetic algorithm selects individuals at random from the current population, considers them as parents use them to produce offspring for next generations. Over the upcoming generations, the population evolves in direction of the optimal solution. In terms of genetic algorithm, an individual indicates one of the solutions and the term population indicates the set of individuals. Genetic Algorithm is better than other conventional methods. Unlike other AI systems, they cannot be broken so easily as there are slight changes in the inputs, or in the presence of noise. In search of a genetic algorithm, a larger state space & multi-modal, offers benefits over various optimization techniques.

B. Simple genetic algorithm

The simple form of GA is as follows:

1. Start with a randomly generated initial population.
2. Calculate the fitness value for each chromosome in the population.
3. Select a pair of parent chromosome from the current population.
4. Perform crossover over the selected site.
5. Mutate the two offsprings.
6. Replace the current population with the new population
7. Go to step 2.

In this paper the following methods are used for implementing genetic algorithm:

An initial population is generated using Simple substitution cipher.

Selection is done based on rank selection method.

Crossover is done using single point crossover.

For the mutation Flipping method is used.

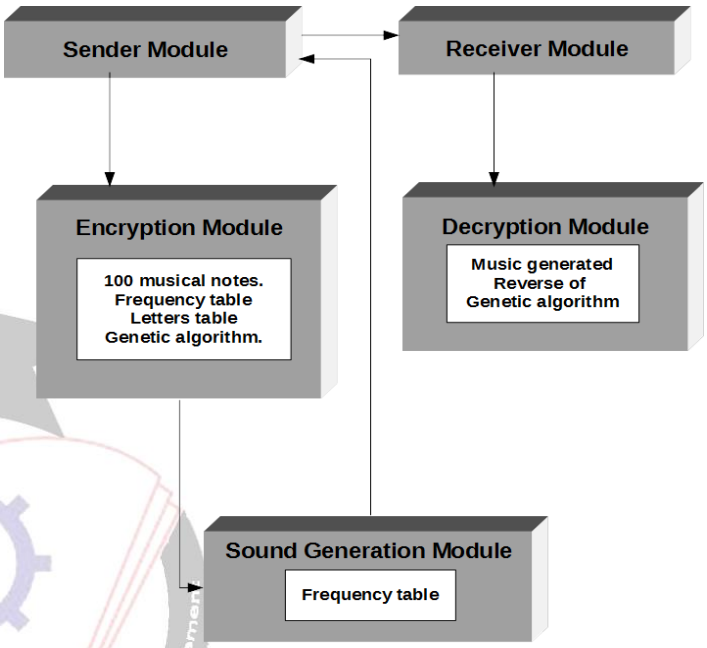

Fig.1-Block diagram of system

C. Encryption

In this system messages are converted into musical notes using substitution cipher and to make the musical piece sound more natural genetic algorithm is being used. Here we consider set of predefined 100 western notes with particular frequency values assigned to each note. Different combinations of these notes are assigned to each alphabet from A to Z. Depending on the letters used in the plain text different combinations of notes for those particular letters are selected. Thus we get the initial population which forms the base for the genetic algorithm. A probability matrix is generated by testing various possible combinations of notes which produce music which sounds more natural. Considering one standard sequence as base, the notes and their corresponding frequency values are stored in the database. A 100 X 100 probability matrix is generated which gives the probability of occurrence of next note after the previous one. Based on this probability matrix fitness value for the initial population is calculated. The two candidates with the highest fitness is selected to perform further operations i.e crossover and mutation. For crossover we use a single site and

for mutation flip the first and last bits. Again the fitness value for both the individuals is calculated and one with the highest fitness is selected as the final encrypted output. The output along with their corresponding frequency values stored in the database is given as the input to the note generation algorithm which generated the actual musical sound. This is implemented using hash map.

D.Decryption

The musical key is taken as an input through which the notes can be obtained and reverse process is used for decryption. In decryption process, the key i.e the text file generated during encryption is taken as an input and the frequency and letter table is used for mapping the musical notes to actual letters of the plaintext. The reverse process of encryption is performed which includes the genesis rules to be performed again in reverse order such as crossover and mutation. At the end of the reverse process, we get the original plain text as output.

IV. CONCLUSION

From the proposed methodology it can be concluded that we can successfully use the musical notes for encrypting the messages. This techniques of using notes makes it more difficult to detect that there is some message hidden in it. And if it is detected that there is a hidden message, the possibility of decryption is very less. As the third person do not have key he/she cannot decrypt it.. So using musical language it is possible to encrypt the message. The permutation and combinations required to decrypt the message makes it nearly impossible provided the intruder doesn't have the key.

ACKNOWLEDGMENT

This research was supported by St. John College of Engineering And Management, Palghar. We are thankful to guide Miss. Linda Mary John who provided expertise that greatly assisted the research and also moderated this paper and in that line improved the manuscript significantly.

We are also grateful to Dr. Satish Taklikar, the principal of SJCET and Prof. Pawan Gujjar, HOD Computer Science for assistance and guidance during the period.

We have to express out appreciation to the Mr. Vaibhav Ambire and Miss. Aditi Raut for sharing their pearls of wisdom with us during the course of this research.

REFERENCES

[1] Ajay Raghav , Baby John. "Musical Cryptography Using Multiple Note Substitution Algorithm", 2016.

[2] Chandan Kumar, Sandip Dutta, Soubhik Chakborty."A Symmetric Key Algorithm for Cryptography using Music", 2013.

[3] Chandan Kumar, Sandip Dutta, Soubhik Chakborty. "Hiding Messages using Musical Notes: A Fuzzy Logic Approach", 2015.

[4] Chandan Kumar, Sandip Dutta, Soubhik Chakborty."Musical Cryptography using Genetic Algorithm", 2014.

[5] M. Yamuna , A. Sankar , Siddarth Ravichandran , V. Harish. " Encryption of a Binary String Using Music Notes and Graph theory", 2013.

[6] Nathan Fortier, Michele Van Dyne ."A Genetic Algorithm Approach to Improve Automated Music Composition", 2011.

[7] Sandip Dutta, Soubhik Chakraborty, N. C. Mahanti. "A Novel Method of Hiding Message Using Musical Notes", 2010

