A Novel Method of Hiding Message Using Musical Notes

Sandip Dutta
Dept. of Information Technology,
Birla Institute of Technology,
Mesra, Ranchi - 835215, India.

Soubhik Chakraborty
Dept. of Applied Mathematics,
Birla Institute of Technology,
Mesra, Ranchi - 835215, India.

N.C.Mahanti
Dept. of Applied Mathematics
Birla Institute of Technology,
Mesra, Ranchi - 835215, India.

ABSTRACT
Security has become an important topic for communication systems. It is a big challenge to provide secure communication in this unique network environment. We propose a novel approach to encrypt a message using musical notes and these musical notes have to be sent by the sender to the receiver. The receiver after receiving the musical notes decrypts it and gets back the original message.

Keywords:
Encryption, Decryption, Musical Notes.

1 INTRODUCTION
Cryptography is basically a study of encrypting (coding) any message that has to be transmitted over a network so that the information is not viewed (and hence, misused) by any unwanted identity. This can be especially of a great use in the present scenario in which the usage of e-commerce, i.e. business over the internet and that too in electronic form has been employed extensively. Cryptography involves encrypting any document by the help of certain algorithms which in turn require simple as well as very complex mathematical concepts for the implementation. The process of encoding the message or the data into some disguised form is called *encryption* and the reverse process of getting back the original message (data) is called *decryption*. Encryption is done with the help of many algorithms and one of such encryption techniques is using a private key and public key. The sender encrypts the message with the help of the public key and the message is sent to the receiver, who in turn decrypts the message with the help of the private key. There are many pros and cons there in such types of algorithms. Cryptography is an important security feature for sending information over a network. Our proposed system can defeat different types of attacks which may come during the transmission of messages over the network. [1]

2 Previous works
The present day encryption algorithms use techniques such as diffusion and confusion to bring about the encryption of data. The process of confusion includes substitution of selected portions of original data by some selected portions of the same piece of data. This means that the original data is converted into an encoded data by using the characters from the original data itself. How to choose the substituted data depends upon the private key which is given alongwith the plaintext (the original document). The process of diffusion includes transposition (more commonly called as the process of permutation). This process, just as the process of confusion, also depends upon the plain text and the private key.

There are three broad classifications of encrypting algorithms. They are: Symmetric, Asymmetric, and Digest algorithms. Symmetric algorithms use the same pair of private key to encrypt and decrypt the plain text into the encrypted data and the encrypted data back to the original plain text and as such they are also called the conventional algorithms. Asymmetric algorithms are those which use different key for encrypting and decrypting purpose. The encrypting is done by public key and the decrypting is done by private key. These algorithms are thus known as public key algorithms. A message digest algorithm works by comparing a hash value which is obtained from the message. This algorithm can be termed as better of the three because of certain sure shot advantages. One of the advantages is that the original message cannot be obtained feasibly from the encrypted message, the other being the infeasibility to construct another message with the same digest. Some of the most popular digest algorithms are Message Digest (md1, md2, md3… etc.) and SHA (the Secure Hash Algorithm) commonly used in mobile networks.
Few works have been done in Biometrics where the keys are generated with the combination of both the sender's and the receiver's fingerprints [2].
Biometric properties of humans, such as their voice, retina, face, eyelid, finger print, etc. can be effective means to achieve protection to the key. In order to access the key, a combination of these biometric characteristics is required to be input for verification. On successful verification, the key can be released[3].
The utterance of the user is represented as a sequence of frames, each having a 12 dimensional vector of cepstral coefficients. A 30 millisecond window of this utterance is specified by the 12-dimensional vector. On capturing the voice completely, there are certain endpoint detection, silence removal and cepstral mean subtraction operations applied. Then a speaker and an independent text acoustic model segment the frame sequence into *m* portions. This is what the algorithm given in reference [4] does.

3 Cryptanalysis and Attacks on Cryptosystems
The art (as can be said if used in the right context) of obtaining the original message from the encrypted message without having the knowledge of the key is known as ***cryptanalysis***. Some of the many techniques available are discussed in the following text.[5]

- **Ciphertext-only attack**: In case where the attacker does not have any information about what the encoded message contains, all information that the attacker has is the encoded text only. In such a scenario, the attacker makes an

intelligent guess as to what can be the plaintext by guessing the fixed format headers. In the past, many attacks have been made by examining the frequency analysis of the ciphertext.

- **Known-plaintext attack**: In this type of attack, the attacker either has a partial knowledge of what the plaintext is, or he can make a guess for some part of the plaintext. The remaining plaintext is obtained by this piece of information. The attacker can determine the key that has been used in the enrypting process and thus crak the code.
- **Chosen-plaintext attack**: in this attack, the attacker attacks the encrypting device by sending any plaintext to the machine and then analysing the encrypted output. Using a very intelligent reasoning, he can very well guess what the key used is and hence succeed in decoding the message.
- **Man-in-the-middle attack**: A technique called packet sniffing is there which can assist the attacker in decoding any information. This is a process in which attacker machines on a network sniff the packets (capture the packet or the data
  streams) over a network. The sniffed packet can be used by the "man in the middle" to obtain the key(s) that two parties are sharing and thus he can very easily decode the entire message without either of the parties having information about this.
  - **Correlation attack:** This attack technique uses the stastical property of correlation between the input (the public key) and the output (the private key or the secret key). The obtained information is used to generate the function that is used in the encrypting process.
  - **Attack against or using the underlying hardware**: There can be an attack on the hardware also. Very intricate examination of the hardware yields characteristics such as the timings of the device, power consumption, radiation patterns etc. These characteristics can later be correlated to obtain the encrypting function. At times, the information can even yield the secret key.
  - **Faults in cryptosystems**: In this condition, there exists some fault in the cryptosystem which might have been the mistake of the programmer. Attackers can thus attack this shortcoming and obtain the necessary information regarding the encrypting function.

4. Encryption / Decryption in Network Security using musical notes (Proposed Scheme)

Our proposed 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 musical notes. These 36 numbers i.e. 26 alphabets and 10 numbers are randomly positioned and then these numbers are assigned musical notes -12 to 23.

Taking the tonic at C conventionally, the twelve notes in the middle octave can be represented by the numbers 0 to 11 respectively. The tonic C of the next higher octave will be assigned the number 12 etc while the note B of the lower octave (before middle) is assigned the number -1 etc. These numbers are actually representing the pitch characterizing the notes. The details are given in table 1 based on ref. [6]. The tonic is the base note or note of origin. All other notes are realized with respect to the tonic. Changing the tonic amounts to changing the scale.

Table 1: Numbers representing pitch of notes in three different octaves

C	Db	D	Eb	E	F	F#	G	Ab	A	Bb	B	**(Notes)**
(lower octave)												
-12	**-11**	**-10**	**-9**	**-8**	**-7**	**-6**	**-5**	**-4**	**-3**	**-2**	**-1**	
(middle octave)												
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	
(higher octave)												
12	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	

We make a rule that first the blank space has to be replaced by zz and then the total message is converted into the number -12 to 23. These numbers have to be converted into vector y and this conversion to vector the required formula which has been used is given below:

$x \in [a, b]$

$a = -12$

$b = 23$

$y=(2x - a - b) / (b - a)$

sound (y,Fs) sends the signal in vector y (with sample frequency Fs) to the speaker available on a computer and even most LINUX platforms. Values in y are assumed to be in the range [-1, 1]. Values outside that range are clipped. Stereo sound is played on platforms that support it when y is an n-by-2 matrix. The values in column 1 are assigned to the left channel, and those in column 2 to the right. The playback duration that results from setting Fs depends on the sound card installed on the machine. Most sound cards support sample frequencies approximately in the range 5-10 kHz to 44.1 kHz. Sample frequencies outside this range can produce unexpected results. The receiver after receiving the sound signal converts into musical note by the formula given below:

$x = a, y = -1$

$x = b, y = 1$

$x = (y * (b - a) + a + b) / 2$

The 36 numbers are positioned randomly in the same manner as it had been done by the sender. The value of x is then decrypted into the original message. The seed value can be changed from time to time according to the understanding between the sender and the receiver.

5 Analysis:

We explain the mechanism of our algorithm with an illustrative example.

Example:

Message : 'Today is Thursday and I have 3 Lectures'

y=['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','0','1','2','3','4','5','6','7','8','9']

B=[-12,-11,-10,-9,-8,-7,-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23]

Randomized Number :
17 12 3 11 27 32 26 29 36 6 10 9
25 33 21 22 34 8 30 18 7 15 28 5
14 24 4 1 20 13 2 31 19 35 16 23

X=14c0xjurlkdb3yv8at62op9zmgewhs5fnq7i

Encrypted Message
5 8 -2 4 1 11 11 23 17 11 11 5 16
-6 -5 17 -2 4 1 11 11 4 20 -2 11
11 23 11 11 16 4 2 14 11 11 0 11
11 -4 14 -10 5 -6 -5 14 17

Converted into sound frequency

-0.02857143 0.14285714 -0.42857143 -0.08571429 -
0.25714286 0.31428571 0.31428571 1.00000000
0.65714286 0.31428571 0.31428571 -0.02857143
0.60000000 -0.65714286 -0.60000000 0.65714286 -
0.42857143 -0.08571429 -0.25714286 0.31428571
0.31428571 -0.08571429 0.82857143 -0.42857143
0.31428571 0.31428571 1.00000000 0.31428571
0.31428571 0.60000000 -0.08571429 -0.20000000
0.48571429 0.31428571 0.31428571 -0.31428571
0.31428571 0.31428571 -0.54285714 0.48571429 -
0.88571429 -0.02857143 -0.65714286 -0.60000000
0.48571429 0.65714286

Table 1 gives the encryption and decryption times. This algorithm runs in O(n) time where n is the number of characters in the message. Fig. 1-5 gives an experimental analysis through "smart statistics". A straight line has evidently captured the trend. *Since time of an operation is actually its weight and a weight-based bound is a statistical bound* (weighing permits mixing of different operations into such a conceptual bound; mathematical count-based bounds are in contrast operation specific), it is important to present the statistical analysis. Moreover the model leads to cheap and efficient prediction which is the motive in computer experiments. Note that mathematical bounds are system independent. A statistical complexity bound can at most be system invariant [7]. Statistical bounds are of two types: probabilistic and non-probabilistic. The one used here is non-probabilistic where the bound is actually *estimated* by providing numerical values to the weights obtained by running computer experiments. No probability statement is made. A probabilistic statistical bound, on the other hand, is one in which a probability statement is made while specifying the bound. When this probability is unity, we get a deterministic bound as its special case [8]. For an extensive literature on computer experiments, [9] may be consulted. See also its review [10].

Table 1: No. of Characters vs. Time

No of Characters in a message	Encryption (Sec.)	Decryption (Sec.)
512	0.0312	0.0156
1024	0.0780	0.0202
1536	0.0936	0.0312
2048	0.1092	0.0468
2560	0.1560	0.0780
3072	0.1716	0.0936
3584	0.1872	0.1248
4096	0.2184	0.1560
4608	0.2808	0.2028
5120	0.3432	0.2340

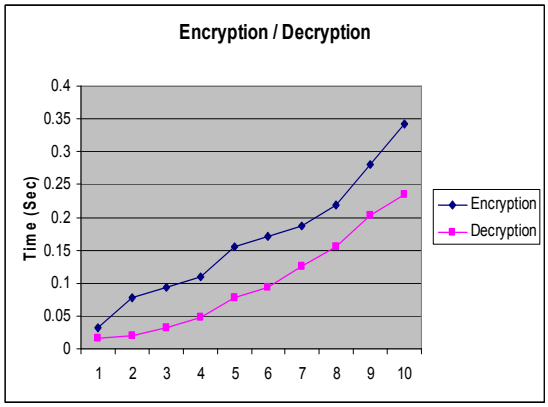

Fig1: Encryption/Decryption times

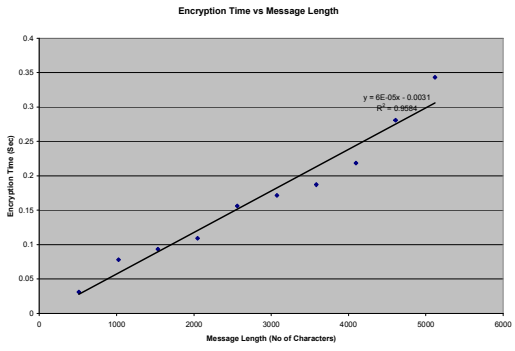

Fig 2: Fitting a straight line to encryption time

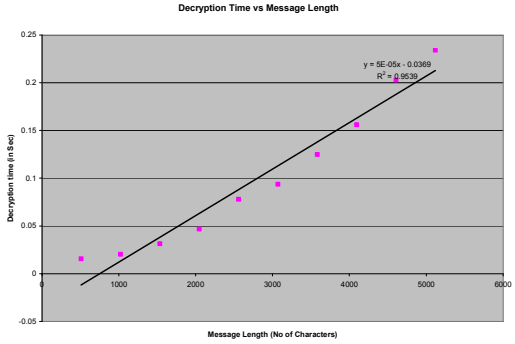

Fig. 3: Fitting a straight line to decryption time

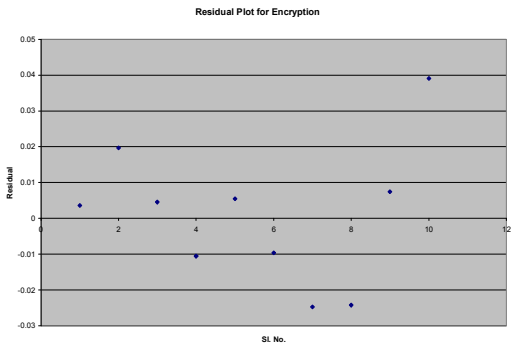

Fig. 4: Residual plot for encryption time straight line fit

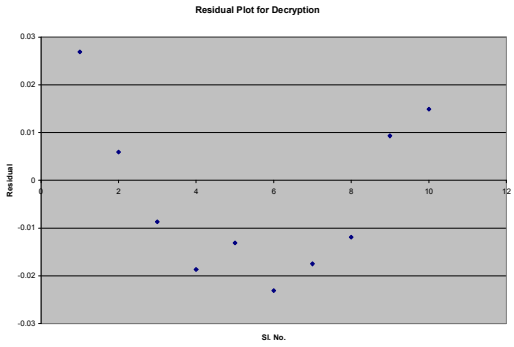

Fig. 5: Residual plot for decryption time straight line fit

6 Defeat attacks

In the light of the attacks that have been discussed, we see that our system is immune to all of those kinds because of the fact that our system uses frequency analysis of the musical note in the encoded sound that is transmitted over the public network.

7 CONCLUSION

Referring to the space and the time complexity, our proposed algorithm is very efficient since it takes very less processing time and storage space. Space is a very important factor for sending any large message over the Internet. The conventional encrypting algorithms require a public key and a private key to encode and decode a message. Our algorithm does not require searching of any such key in any such public domain or any private domain, which again preserves a lot of time which is used in locating the keys. Very large message, including image can be sent with the help of this proposed argument.

REFERENCES

[1] M. Tolga Sakalli, Ercan Bulu$ and Fatma Buyuksaracoglu, "Cryptography Education for Students",0-7803-8596-9/04 IEEE, 2004

[2] Sandip Dutta, Avijit Kar, N.C.Mahanti and B.N. Chatterji, "Network Security Using Biometric and Cryptograpy ", ISBN 978-3-540-88457-6, Springer, 2008, P38-44

[3] Alper Kanak, Gebze Yüksek Teknoloji Enstitüsü, "Biometrics for computer security and cryptography",June 3rd, 2004

[4] F. Monrose, M. K. Reiter, Q. Li, S. Wetzel "Using voice to generate cryptographic keys: A position paper", Proc. Of Odyssey 2001, The Speaer Verification Worshop, June 2001.

[5] Handbook of Applied Cryptography by Menezes, van Oorschot, and Vanstone and Applied Cryptography by Schneier.

[6] S. Chakraborty, K. Krishnapriya, Loveleen, S. Chauhan and S. S. Solanki, *Analyzing the Melodic Structure of a North Indian Raga: a Statistical Approach*, Electronic Musicological Review, vol. XII, 2009

[7] S. Chakraborty, S. K. Sourabh , *On Why an Algorithmic Time Complexity Measure can be System Invariant rather than System Independent*, Applied Math. and Compu,Vol. 190(1), 2007, p. 195-204

[8] S. Chakraborty, Review of the book *Computational Complexity*: *A Conceptual Perspective* (Ist Ed.) by O. Goldreich, Cambridge University Press, N. Y. 2008, published in Computing Reviews, April 27, 2009 (www.reviews.com)

[9] K. T. Fang, R. Li and A. Sudjianto, *Design and Modeling of Computer Experiments*, Chapman and Hall, 2006

[10] S. Chakraborty, Review of [9] published in Computing Reviews, Feb 12, 2008(www.reviews.com)