Design of a Fuzzy Rule Based Expert System for Automatic Raga Selection for Cryptographic Applications

Prashant Pranav (prashantpranav19@gmail.com)
Birla Institute of Technology https://orcid.org/0000-0002-3932-3048
Sandip Dutta
Birla Institute of Technology

Research Article

Keywords: Music, Cryptography, Fuzzy set, Indian raga, encryption, decryption

Posted Date: February 23rd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1163172/v1

Abstract

Strengthening the security of data and information of an organization or an individual is of utmost importance in the current scenario. Due to the increasing computing power of the intruder, the need for an emerging and new technique to secure the messages cannot be denied. The unbreakable of the future may be broken with some effort and time. We have proposed a new technique to secure the information which uses the employment of a *Fuzzy Expert System* in the *Hindustani Music* to produce encrypted sequences in the form of musical notes. These produced note sequences can be sent over the communication medium in the form of a piece of music. This work is basically an extension of our work proposed in [1]. We have simulated three Hindustani ragas viz. Yaman Kalyan, Bageshree and Malkuan with fuzzy rules to select a new raga for messages of different length.

1. Introduction

Security is one of the key requirements in today's era of technological progress. It is necessary to provide security measures to protect the confidential information of individuals and organizations. With the help of many existing security protocols, it can be ensured that confidential data and messages transmitted through any medium are not affected by any adversary. But is the existing security protocol sufficient? There are many vague answers to this contradictory question. Some people emphasize that the security provided by third parties to organizations or individuals or the security embedded in the applications or processes they use is not affected by spies. The other group emphasized that the existing security-providing protocols need continuous and gradual improvement to cope with the adversary's computing power. As computing shifts from traditional methods to more quantum-oriented methods, the need to develop algorithms suitable for quantum computers is the current research need in the field of cryptography and network security. Cryptography is basically the formulation of mathematical models to provide security. Cryptography is one of the key requirements (not the only requirement) to provide security. Ensure that messages or data transmitted through any unsafe means are unreadable and unbreakable.

1.1. Fuzzy Set and Fuzzy Rule Based Expert System

Introduced in [1] by Zaldey, the Fuzzy set theory allows one to define some intermediate values like true or false, good or bad, low, medium or high in addition to the traditional values. In contrast to the classical set theory which allows values to either belong to a set or not, fuzzy logic assigns a membership function for values which varies between the interval [0, 1]. The paper uses a Triangular Fuzzy Number (TFN) which can be represented simply by (l, m, u) where ‘l’ represents “low”, ‘m’ represents “medium” and ‘h’ represents “high”. Membership function of a TFN can be shown as follows:

$$\mu_M(x) = \begin{cases} 0 & x < 1 \\ \frac{x-l}{m-l} & 1 \le x \le m \\ \frac{u-x}{u-m} & m \le x \le u \\ 0 & x > 1 \end{cases}$$

where, $\mu_M(x)$ is the membership function.

An expert system is the computer aided system that emulates the behavior of human experts in a well defined manner. A fuzzy expert system makes the use of fuzzy membership functions and the defined fuzzy rules to simulate something about a data or a process. A fuzzy expert system follows the following general convention for formulating fuzzy rules:

If A is High and B is Medium, Then C= Low

where A and B are input variables

C is the output variable

2. Related Work

Using music for confidential purposes is a new genre, and there has been little research in this area so far. In [2], a symmetric key algorithm using music is proposed. Each character in the message corresponds to a note in the three octaves. [3] shows the use of musical notes to hide information. [4] proposed a hybrid Polybius-Playfair encryption system, which focuses on first encrypting the message with Playfair encryption and then re-encrypting it with Polybius encryption. Polybius passwords use musical notes instead of information. In [5], a method based on fuzzy logic is used to generate a good musical sequence. The article proposes a symmetric key replacement cipher, in which each character is replaced with a candidate note. The use of genetic algorithms to generate the best sequence is shown in [6]. Through a genetic algorithm, the most suitable grade for this purpose is raised to a new level. Some famous works in computational musicology are attributed to (7 and 8). In [7], a system is shown that extracts audio files into their constituent note sequences and classifies the raga used by extracting Arohana and Avarohana patterns. Artificial neural networks can also be used to make artificial music. [8] proposed a neural network-based method to generate various combinations in any range. The article also introduces Indian music in detail. Learning the complete musical model through the recurrent neural network has not been successful. Therefore, [9] proposed to use the recurrent neural network LSTM for the same purpose. Statistical analysis of Indian music is shown in (9 and 10). [9] shows a statistical method for modeling Indian classical music. The paper demonstrated a probabilistic method for the detection of notes and demonstrated the rapid stabilization of the relative frequencies of the most

important notes in any Rager structure. Raga is a melodic structure with fixed notes and a set of rules that are used to characterize specific emotions conveyed by the performance [12]. In [13], a statistical analysis of old songs using Raga Bhairavi is shown.

3. Proposed Approach: Design Of A Fuzzy Rule Based Expert System For Automatic Raga Selection For Cryptographic Applications

We have incorporated the use of SNCA algorithm with fuzzy rules to select a different raga for messages of different lengths. To decide which raga to be used for which specific message length we have computed the execution time of three well known Indian ragas namely Yaman Kalyan, Bageshree and Malkauns to see which raga best suits for which message length. In our fuzzy rules, we have used only one input variable in the form of execution time of each raga and one output variable in the form of raga selection. In the following section we discuss about the SNCA algorithm and the run time of the three ragas for messages of different lengths. For a proper description of the algorithm readers are encouraged to see [1]

We simulated the sequence of raga Yaman Kalyan, Bageshree and Malakun using the SNC algorithm. For the simulation purpose we have used the following notation corresponding to the notes of Hindustani music.

Sa – S, Komal Re- r, Shudh Re- R, Komal Ga- g, Shudh Ga- G, Pa-P, Komal Dha-d, Shudh Dha-D,Komal Ni- n, Shudh Ni- N, Sudh Ma- M, Tivra Ma- m

For the TPM and Class Matrix of Raga Yaman Kalyan see [1]

Next, using the same mechanism, we have constructed the TPM and Class Matrix of Bageshree and Malkauns as shown in Table 1, 2, 3 and 4 below

Table 1
TPM of Bageshree

	S	R	G	M	P	D	n
S	6/46	7/46	0/46	10/46	0/46	5/46	18/46
R	12/17	0/17	0/17	0/17	0/17	0/17	5/17
g	0/20	9/20	1/20	10/20	0/20	0/20	0/20
M	1/45	0/45	16/45	2/45	5/45	16/45	5/45
P	0/5	0/5	0/5	0/5	0/5	5/5	0/5
D	10/58	1/58	3/58	23/58	0/58	2/58	19/58
n	17/48	0/48	0/48	0/48	0/48	30/48	1/48

Table 2
Class Matrix of Bageshree

	S	R	g	M	P	D	n
S	0-6/46	6/46-13/46	13/46-13/46	13/46-23/46	23/46-23/46	23/46-28/46	28/46-46/46
R	0-12/17	12/17-12/17	12/17-12/17	12/17-12/17	12/17-12/17	12/17-12/17	12/17-17/17
g	0-0/20	0/20-9/20	9/20-10/20	10/20-20/20	20/20-20/20	20/20-20/20	20/20-20/20
M	0-1/45	1/45-1/45	1/45-17/45	17/45-19/45	19/45-24/45	24/45-40/45	40/45-45/45
P	0-0/5	0/5-0/5	0/5-0/5	0/5-0/5	0/5-0/5	0/5-5/5	5/5-5/5
D	0-10/58	10/58-11/58	11/58-14/58	14/58-37/58	37/58-37/58	37/58-39/58	39/58-58/58
n	0-17/48	17/48-17/48	17/48-17/48	17/48-17/48	17/48-17/48	17/48-47/48	47/48-48/48

Table 3
TPM of Malkauns

	S	g	M	d	N
S	6/55	4/55	9/55	17/55	19/55
g	11/43	1/43	26/43	1/43	4/43
M	0/62	37/62	7/62	14/62	4/62
d	4/49	1/49	19/49	0/49	25/49
n	34/52	0/52	1/52	17/52	0/52

Table 4
Class Matrix of Malkauns

	S	g	M	d	N
S	0-6/55	6/55-10/55	10/55-19/55	19/55-36/55	36/55-55/55
g	0-11/43	11/43-12/43	12/43-38/43	38/43-39/43	39/43-43/43
M	0-0/62	0/62-37/62	37/62-44/62	44/62-58/62	58/62-62/62
d	0-4/49	4/49-5/49	5/49-24/49	24/49-24/49	24/49-49/49
n	0-34/52	34/52-34/52	34/52-35/52	35/52-52/52	52/52-52/52

To formulate fuzzy rules we first have to compare the execution time for encryption and decryption of the three ragas. We compared the execution time for encryption of the three ragas with RSA and AES-128. The result of the execution time has been shown in the below Table 7. Figure 3, 4, 5, 6, 7 and 8 below represents the fitted line plot of the tabulated values.

Table 7
Comparison of Encryption Time for the Raga Bageshree, Yaman Kalyan and Malkauns with AES and RSA

Input (In Bytes)	Yaman Kalyan	Bageshree	Malkauns	RSA	AES-128
16	0.002574	0.000681	0.023533	0.036797	0.02912
32	0.002679	0.001041	0.0542	0.038213	0.05924
48	0.003652	0.001276	0.085867	0.041075	0.08768
64	0.005709	0.001583	0.1147	0.051853	0.12452
80	0.005985	0.001911	0.142367	0.055544	0.14292
96	0.006326	0.002536	0.170833	0.064573	0.17168
112	0.006712	0.002907	0.203233	0.069025	0.20656
128	0.00716	0.002983	0.232333	0.070041	0.2421
144	0.007832	0.003293	0.2653	0.0827	0.26446
160	0.008112	0.003368	0.301	0.088028	0.32652
176	0.008325	0.004253	0.317767	0.092715	0.32386
192	0.008869	0.005369	0.348833	0.098436	0.39026
208	0.009268	0.005985	0.4473	0.12118	0.44104
224	0.009825	0.006325	0.4853	0.180937	0.47304
240	0.009912	0.006741	0.528	0.191909	0.50372
256	0.01082	0.007012	0.553733	0.20132	0.5117
320	0.0133124	0.007642	0.6325	0.2875	0.7824
384	0.0153607	0.008129	0.7521	0.3157	0.8291
448	0.0169732	0.008836	0.8256	0.3966	1.1285
512	0.0160022	0.009131	0.8925	0.4255	1.3689

The fitted line plot clearly shows that the three ragas take comparatively less amount of time as compared to the execution time of AES-128 and RSA. Among the three ragas, raga Malkaun takes the largest amount of time for encryption followed by raga Yaman Kalyan and raga Bageshree. So, for

securing large amount of data using our SNCA algorithm, raga Bageshree is the most suitable. Similarly, for medium amount of data, raga Yaman Kalyan is a better option and for securing small amount of data, raga Malkaun can be used. Based on the above discussion, we have formulated three different fuzzy rules as discussed below:

R1. *If "Message Length" is small Then select Raga Malkaun*

R2. *If "Message Length" is medium Then select Raga Yaman Kalyan*

R3. *If "Message Length" is large Then select Raga Bageshree*

Further, to send the messages in the form of music, so as to defy the intruder of sensing any confidential information is being sent over the network, we have used the Chebyshev's inequality as used in [1], to calculate the duration of each note in the three different raga. Frequency of each note has been set to the default frequency as used in Hindustani music. The computed duration of each note of the three ragas has been shown in the below Table 8, 9 and 10.

Table 8
Duration and Frequency of Raga Yaman Kalyan

Notes	Duration (Neglecting negative parts)	Frequency (in Hz)
S	(0-1.7813)	240
R	(0-2.3830)	248
G	(0-2.8834)	284.4
P	(0-3.4924)	360
D	(0-1.8690)	379
M	(0-4.511)	320
N	(0-2.9028)	376
m	(0-0.9815)	337.5

Table 9
Duration and Frequency of Raga Bageshree

Notes	Duration (Neglecting negative parts)	Frequency (in Hz)
S	(0-2.342)	240
R	(0-1.523)	248
g	(0-2.225)	303
M	(0-3.435)	320
P	(0-1.712)	360
D	(0-3.169)	379
n	(0-4.025)	450

Table 10
Duration and Frequency of Raga Malkaun

Notes	Duration (Neglecting negative parts)	Frequency (in Hz)
S	(0-1.273)	240
M	(0-3.526)	248
g	(0-2.358)	303
n	(0-4.053)	450
D	(0-1.874)	376

The figures in figure 9, 10 and 11 shows the attained frequency of ragas Malkuan, Bageshree and Yaman Kalyan as the message gets encrypted and is composed in the form of music.

4. Conclusion

The proposed expert system using fuzzy logic selects a new raga for messages of different lengths. The selected raga is run through the SNC algorithm and then using the Chebysev's inequality, is incorporated with the duration and pre-defined frequencies of each note to send the messages in the form of a piece of music. This defies the intruder of sensing any confidential information is being sent over the network. Selection of a new raga on every run further strengthens our work as the present note in every raga is different and of varying duration.

Declarations

Ethical approval: The authors declare that the manuscript complies with the ethical standards of the journal.

Funding Details: The authors declare that they have not received any funding for this research.

Conflict of Interest: The authors declare that they not have any conflict of interest.

Informed Consent: The authors gives right to the journal for all the process related to the handling of the manuscript.

Author Contributions: All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Prashant Pranav and Sandip Dutta. The first draft of the manuscript was written by Prashant Pranav and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Competing Interest: The authors have no relevant financial or non-financial interests to disclose.

Data Availability: Data may be made available upon request.

References

1. Pranav P, Chakraborty S, Dutta S (2019), A new cipher system using semi natural composition in Indian raga, Soft Comput (2020), 24:1529–1537 https://doi.org/10.1007/s00500-019-03983-8(0123456789().,-volV)(0123456789,-().volV)
2. Dutta S, Kumar C, Chakraborty S (2013) A symmetric key algorithm for cryptography using music. Int J Eng Technol 5(3):3109–3115
3. Kumar C, Dutta S, Chakraborty S (2015b) Hiding messages using musical notes: A fuzzy logic approach. Int J Sec Its Appl
4. Kumar C, Dutta S, Chakraborty S (2015a) A hybrid polybius–playfair music cipher. Int J Multimed Ubiquitous Eng 10(8):187–198
5. Kumar C, Dutta S, Chakraborty S (2015b) Hiding messages using musical notes: A fuzzy logic approach. Int J Sec Its Appl 9(1):237–248
6. Kumar C, Dutta S, Chakraborty S (2014) Musical cryptography using genetic algorithm. In: Paper presented at the International conference on circuit, power and computing technologies (ICCPCT), pp 1742–1747
7. Shetty S, Achary K (2009) Raga mining of Indian music by extracting arohana–avrohana pattern. Int J Curr Trends Eng Technol
8. Sinha P (2008) Artificial composition: an experiment on north Indian music. J New Music Res 37(3):221–23
9. Eck D, Schmidhuber J (2002) A first look at music composition using LSTM recurrent neural networks. Technical Report No. IDSIA- 07-02
10. Chakraborty S, Solanki S, Roy S, Chauhan S, Tripathy S, Mahto K (2008) A statistical approach for modelling Indian classical music. Achieve of Cornell University e-Library. http://arxiv.org/

abs/0809.3214

11. Chakraborty S, Shukla R, Krishnapriya K, Loveleen Chauhan S, Kumari M, Solanki S (2009) A statistical analysis of a raga based song. Georgian Electron Sci J Musicol Cult Sci 2(4):21–33
12. Chakraborty S, Mazzola G, Tewari S, Patra M (2014) Computational musicology in Hindustani music. Springer, Berlin
13. Chakraborty S, Kalita M, Kumari N (2011) Semi-natural composition: an experiment with north Indian ragas. Int J Comput Cognit 9(2):51–5

Figures

Figure 1

Figure 3. Input vs Execution Time for the Raga Yaman Kalyan, Bageshree, Malkaun, RSA and AES-128.

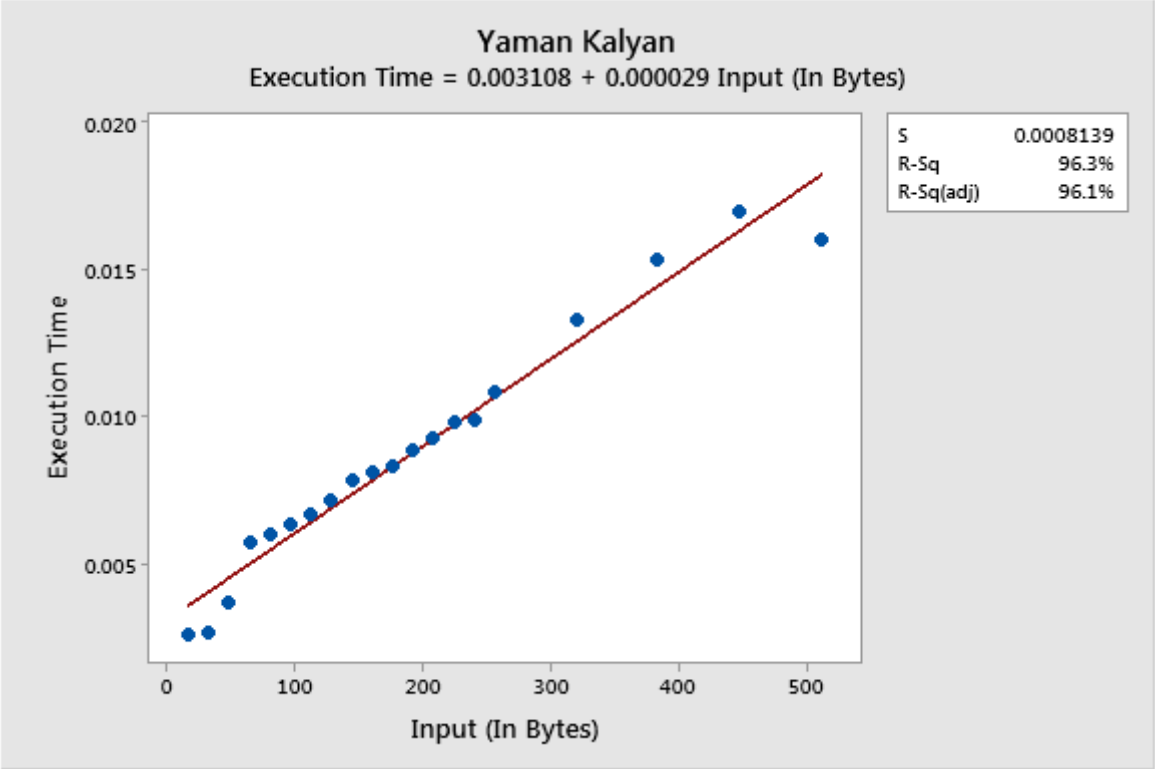

Figure 2

Figure 4. Fitted Line Plot of Raga Yaman Kalyan

Figure 3

Figure 5. Fitted Line Plot of Raga Bageshree

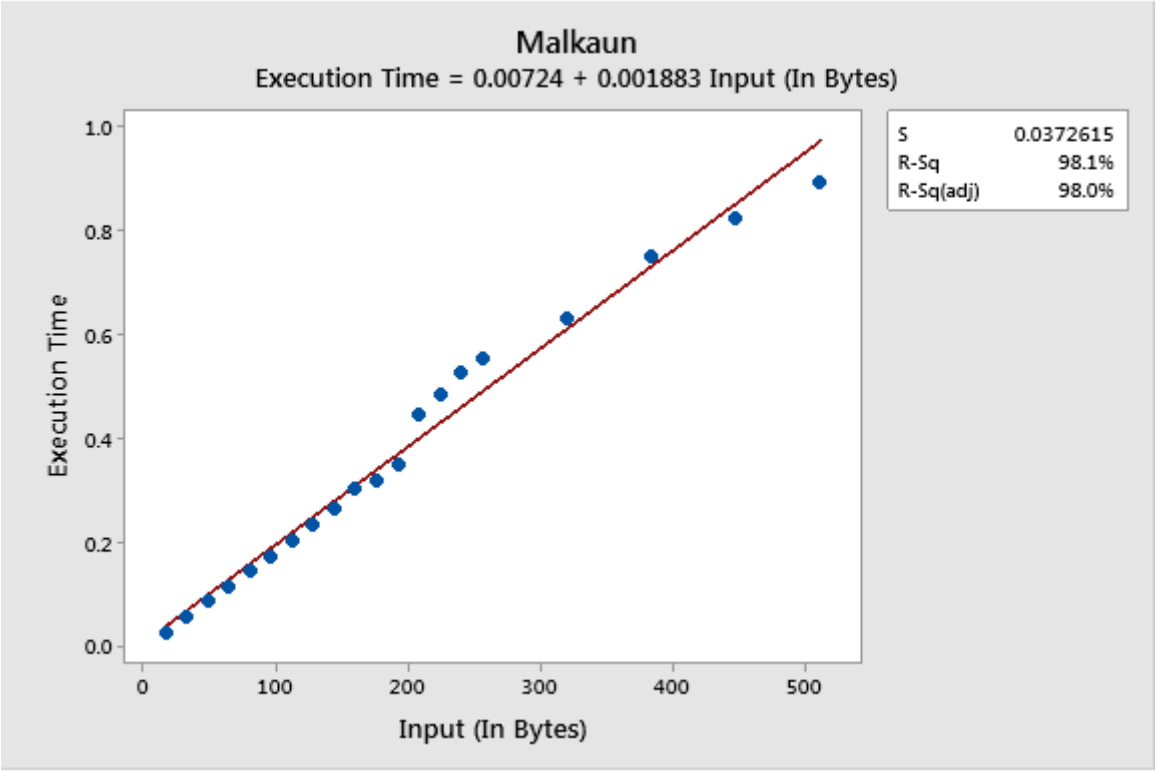

Figure 4

Figure 6. Fitted Line Plot of Raga Malkaun

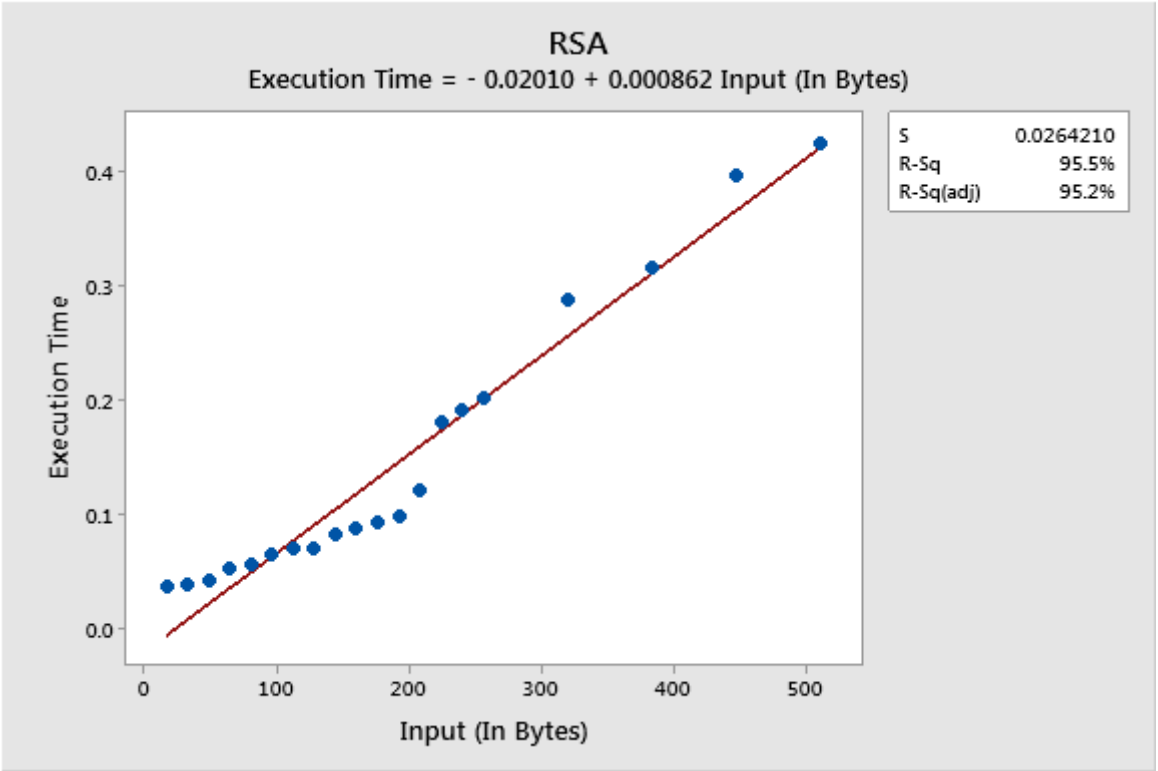

Figure 5

Figure 7. Fitted Line Plot of RSA

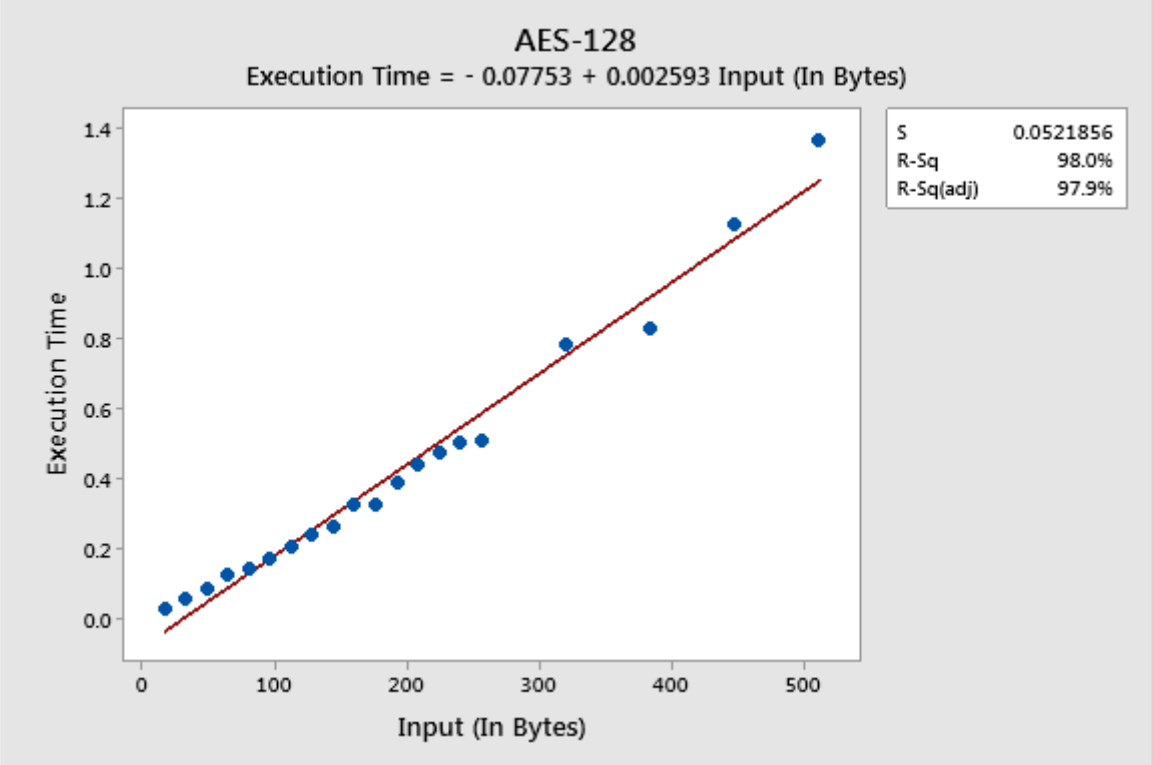

Figure 6

Figure 8. Fitted Line Plot of AES-128

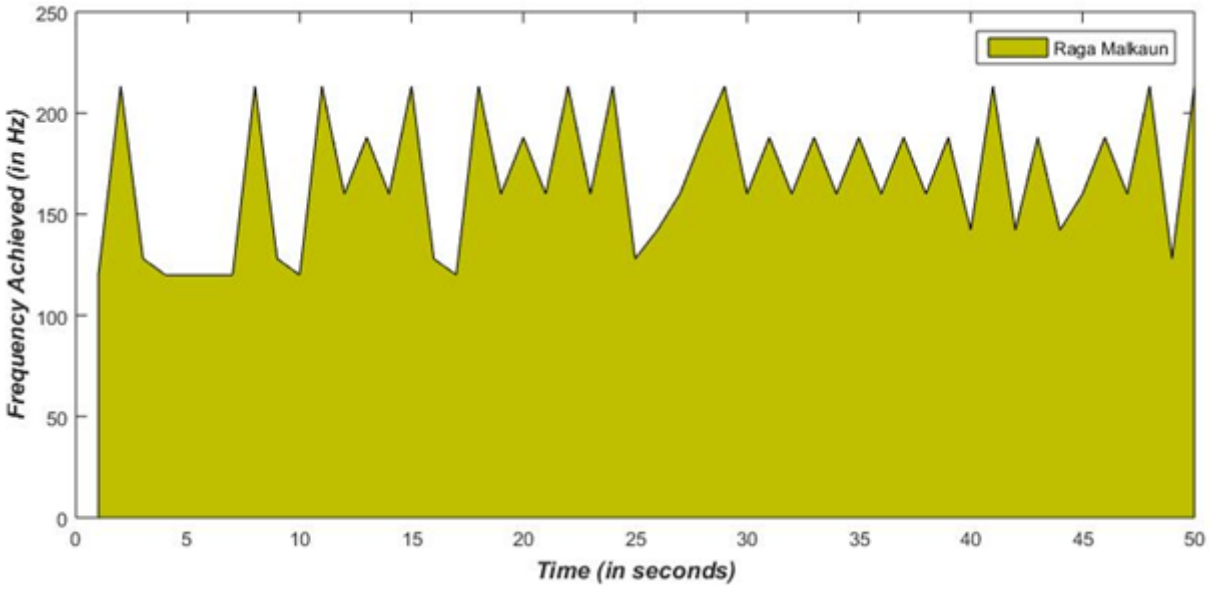

Figure 7

Figure 9. Attained Frequency of Raga Malkaun

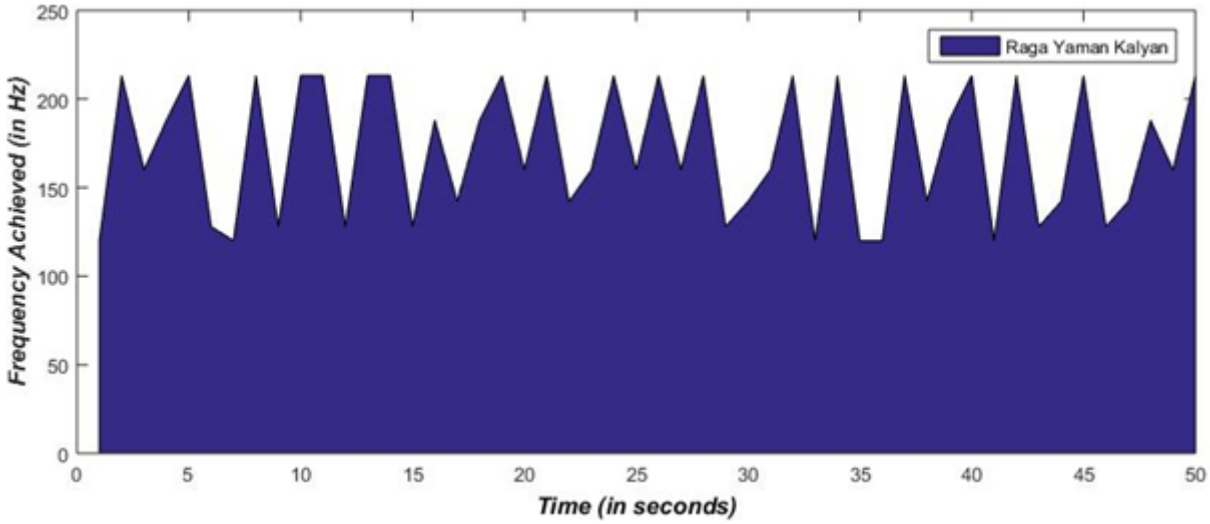

Figure 8

Figure 10. Attained Frequency of Raga Yaman Kalyan

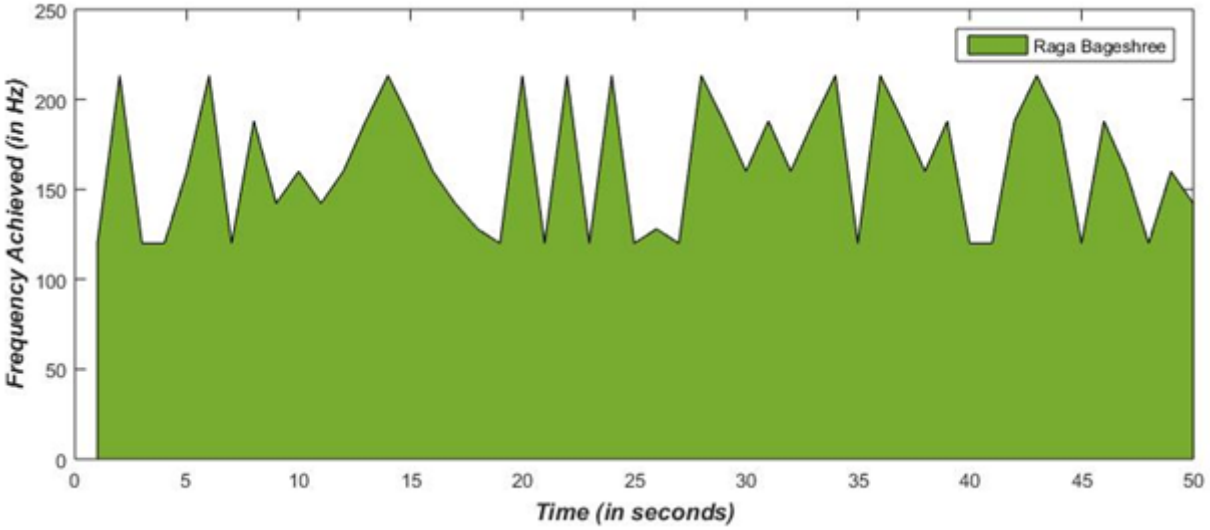

Figure 9

Figure 11. Attained Frequency of Raga Bageshree