Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.140 – 149

RESEARCH ARTICLE

Automated Cryptanalysis of Transposition Ciphers Using Cuckoo Search Algorithm

[1] Morteza Heydari*,[1] Mahdieh Nadi Senejani

[1]Department of Computer Engineering, College of Computer Science, Ashtian Branch,

Islamic Azad University, Ashtian, Iran

*E-mail: morteza2@gmail.com

Abstract

An approach of information security is Cryptography.Cryptanalysis is the science study to break cryptography without the encryption key. The present paper shows the benefits of the implementation of a novel genetic algorithm, the "Cuckoo Search" Algorithm (CSA) with new fitness function for the cryptanalysis of transposition cipher. The fitness function is evaluated based on the most common bigrams and trigrams. Results show that the algorithm proposed in this paper is effective for cryptanalysis of transposition cipher with long key lengths up to 30 due to its strong reliability and fast convergence speed.

[1]**Corresponding Author:** Morteza Heydari, Department of Computer Engineering, Ashtian Branch, Islamic Azad University, Ashtian, Iran. E-mail: morteza2@gmail.com - phone numbers:+9809133612974

Keywords: "Cuckoo Search" Algorithm (CSA), Cryptanalysis, Encryption key, Transposition Cipher.

1. Introduction

There are different ways to secure information passed over the network.Cryptology is at the heart of providing such guarantee. That is the science of building and analyzing different encryption and decryption methods. Cryptology consists of two subfields; Cryptography & Cryptanalysis. Cryptanalysis is the science and study of method of breaking cryptographic techniques i.e. ciphers. The cryptanalysis can at maximum guess the key in which case a very large number of guesses for the key to be correct can ensure the near unbreakability of the cipher [1]. Many types of classical ciphers exist, although most fall into one of two broad categories: substitution ciphers and transposition ciphers. A transposition cipher the plaintext remains the same, but the order of characters is shuffled around. However, if the key is short and the message is long, then various cryptanalysis techniques can be applied to break such ciphers. In a simple columnar transposition cipher, the plaintext is written horizontally onto a piece of graph paper of fixed width and the cipher text is read off vertically [2]. It works by splitting the plain text into fixed sized blocks. The length of the key (also called the period) is the same as the size of the block. Letters in each block are permuted according to a same pattern (the key) [3]. In Table 1 is shown the key and the encryption process of the previously described transposition cipher.

Table 1. Example of the transposition cipher key and encryption process

	1	4	3	5	8	7	2	6
Key:	C	O	M	P	U	T	E	R
Plain:	C	R	Y	P	T	A	N	A
	L	Y	S	I	S	U	S	I
	N	G	I	M	P	R	O	V
	E	D	G	E	N	E	T	I
	C	A	L	G	O	R	I	T
	H	M	A	B	C	D	E	F

Plain Text : CRYPTANALYSIS USING IMPROVED GENETIC ALGORITM
Cipher Text : CLNECHNSOTIEYSIGLARYGDAMPIMEGBAIVITFAURERDTSPNOC

Recently there has been a call for non-standard approaches, including many algorithms such as particle swarm optimization, cuckoo search and firefly algorithm, to be applied to cryptography problems. A newly developed algorithm described based on the breeding behavior of cuckoo birds. The "Cuckoo Search" Algorithm (CSA) developed by Yang and Deb [4-5], is a new meta-heuristic algorithm imitating animal behavior. In CSA, each egg in a nest represents a solution, and a cuckoo egg represents a new solution. The aim is to use the new and potentially better solutions (cuckoos) to replace a not-so-good solution in the nests. In the simplest form, each nest has one egg. The algorithm can be extended to more complicated cases in which each nest has multiple eggs representing a set of solutions [4-5]. The works of Yang & Deb [4-5], Civicioglu & Besdok [6], Rajabioun [7] and Valian et al. [8] further confirmed that the “cuckoo search” algorithm, in its original or improved version, proves to be very effective. The method has been successfully tested on a large number of benchmark functions of varied dimensions and difficulty levels.

In this paper, the cryptanalysis of transposition cipher by applying CSA is presented. The improved fitness function is used based on the most common bigrams and trigrams. Numerical examples show that the proposed algorithm has satisfied global performance, high convergence speed, minimum error, stable convergence performance and successful in breaking the cipher with key lengths up to 30.

The paper is organized as follows. Section 2 presents a brief description of basic CSA process. In section 3 is presented new method for Cryptanalysis of Transposition Cipher by applying CSA. In this section, the assumptions used in its evaluation function algorithm is introduced and presented. The results presented in Section 4 and finally Section 5 presents the conclusion of this study.

2. Basics of the CSA

The Cuckoo Search Algorithm (CSA) is based on the breeding behavior of the Common Cuckoo. This species lays its eggs in foreign nests where the deceived host bird incubates the cuckoo egg and feeds the chick. In some cases a host bird is able to distinguish between its own and the cuckoo's egg. In this situation, the discovered egg might be thrown off the nest, or the nest will be abandoned completely to build a new one somewhere else. Furthermore, some cuckoos, in anticipation of this unwelcoming reaction, evolved their parasitic behavior by concentrating on imitating the eggs of specific host birds. An additional feature of the Common Cuckoo's reproduction strategy is the timing of the hatching: the cuckoo chick will usually hatch first, and then it throws the host eggs out of the nest securing enough feeding for it. Various studies have shown that the flight behavior of many animals and insects demonstrates the typical characteristics of Lévy flights [4-5, 9-12]. A Lévy flight is a random walk in which the step-lengths are distributed according to a heavy-tailed probability distribution. After a large number of steps, the distance from the origin of the random walk tends to a stable distribution. The CSA is mainly based on the generation of new solutions via Lévy flights which are based on a Lévy distribution. Figure 1 illustrates the basic steps of the CSA.

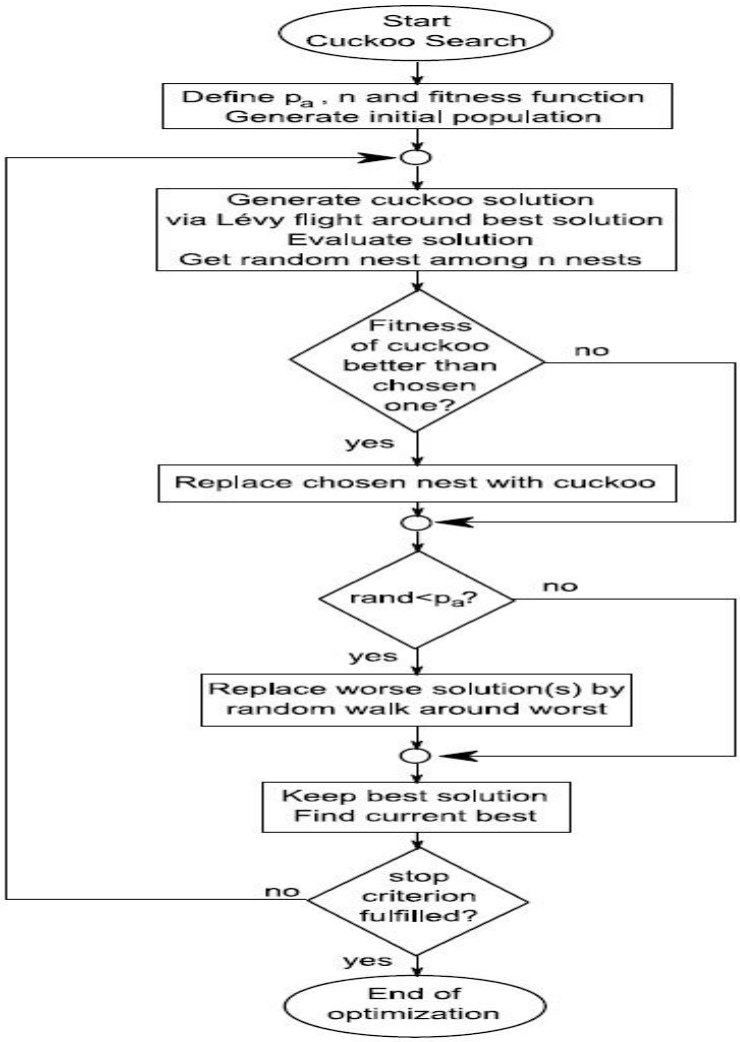

Figure 1. Flow chart of the basic procedure of the CSA (based on [4] and [13])

3. The proposed method using CSA

3.1 Generating initial cuckoo habitat

The variable arrays in CSA, it is called "habitat" and sample array is defined as follows in Equation (1):

$$habitat = \left[x_{i=1}, x_{i=2}, x_{i=3}, ..., x_{i=N} \right] \quad (1)$$

Xi=between 1 to estimated key length

N= square of estimated key length.

3.2 profit function

Most researchers use fitness functions which combine unigram, bigram and trigram frequency statistics. In this research uses bigram and trigram models. Equation 2 is used as profit function:

$$F_p = \alpha \sum_{i=1}^{6} C_i . B_i + \beta \sum_{j=1}^{4} D_j . T_j \quad (2)$$

Where, Ci and Dj denotes the frequency of the bigram and trigram letters respectively, where 1<i<6 and 1<j<4. Also, Bi and Tj denotes the array of most common the bigram and trigram letters respectively. Table 2 shows the fitness weight table used in this research.

Table 2. The fitness weight table proposed in this research

Bigram	Score
TH	2
HE	1
IN	1
ER	1
AN	1
ED	1

Trigram	Score
THE	5
ING	5
AND	5
EEE	-5

α and β allow assigning of different weights to each of the bigram and trigram types respectively, where α + β =1. According to figure 2 the best values of α and β are 0.7 and 0.3 respectively.

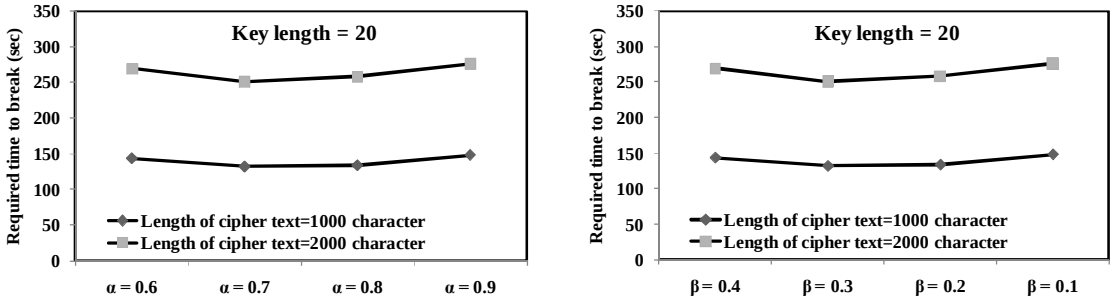

Figure 2. Time Comparison of values α and β for different transposition size

4. Results and Discussion

In this section, the performance of the proposed CSA algorithm is extensively investigated by a large number of experimental studies. All computational experiments are conducted with Visual C# program. Performance evaluation and analysis of this algorithm were operated on diverse texts encrypted with kinds of keys. Table 3 shows results for amounts of cipher text ranging from 500 to 2000 characters. For each size there are some keys have been broken fully. If the cipher text is having more size the breakable key and success rates is more, however, the time of cryptanalysis increase.

Table 3. The amount of key recovered Versus Transposition Size Using different Cipher Text Characters

Cipher length = 500 characters																
Key Size	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Key Recovered	17	18	19	20	21	22	23	23	23	24	24	24	25	26	26	27
Cipher length = 1000 characters																
Key Size	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Key Recovered	17	18	19	20	21	22	23	24	25	26	27	27	28	28	28	29
Cipher length =2000 characters																
Key Size	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Key Recovered	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	31

Figure 3 illustrates the cost function minimization of the proposed CSA for different key lengths (20 and 30 keys) and different cipher text length (500, 1000 and 2000) to attack transposition cipher.

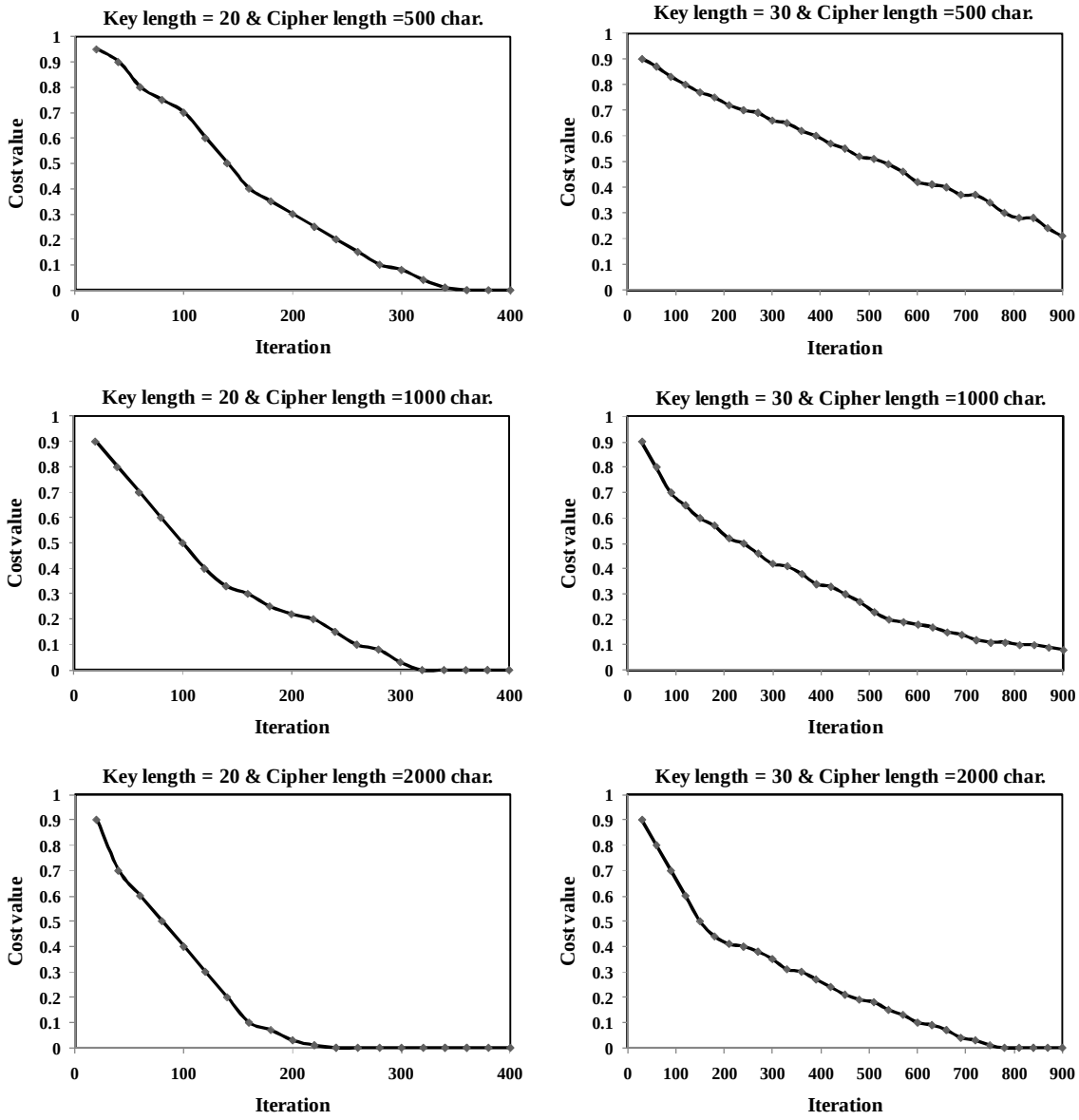

Figure 3. The cost function minimization comparison of algorithm with different cipher text length and key length

Seeing from figure 3, it can be found that with increasing the amount of cipher text and same key length, the rate of cost function minimization of algorithm increases and the speed of convergence is high. Also, with increasing the amount of key length in same cipher text, the numbers of iterations increases. This result shows the key length has a more impact than the cipher text characters on accuracy and convergence proposed algorithm. This demonstrates the importance of key length.

5. Conclusion

Recently introduced cuckoo search algorithm (CSA) has proven its excellent capabilities, such as faster convergence and better global minimum achievement. In this paper, an improvised CSA was presented for the cryptanalysis of transposition cipher with long key lengths. The fitness weights used in fitness function CSA were 0.0 for unigrams, 0.7 bigrams and 0.3 for trigrams. Experimental results indicated that this improved fitness function is extremely powerful technique for an attack on transposition cipher. Amount of recovered key in transposition cipher using this algorithm is more than the other techniques. The performance of the algorithm is found to be better and considerably faster than exhaustive search and other existing methods.

References

[1]. Garg, P. and Sherry A.M. 2007. An Improved Cryptanalytic Attack on Knapsack Cipher using Genetic Algorithm, International Journal of Information and Communication Engineering, 3(6): 444-451.

[2]. Sokouti, M. Sokouti, B. and S. Pashazadeh.2009. An approach in improving transposition cipher system, Indian Journal of Science and Technology, 2(8): 9-15.

[3]. Chen, J. 2010. Decrypting Classical Cipher Text Using Markov Chain Monte Carlo, STA4000 Report.

[4]. Yang, X.S., Deb, S.2009. Cuckoo search via Lévy flights, Proceeings of World Congress on Nature & Biologically Inspired Computing, India, 210-214.

[5]. Yang, X.S., Deb, S. 2010. Engineering Optimization by Cuckoo Search, Int. J. Mathematical Modelling and Numerical Optimisation, 1(4): 330–343.

[6]. Civicioglu, P. & Besdok, E. 2011. A conceptual comparison of the Cuckoo-search, particle swarm optimization, differential evolution and artificial bee colony algorithms, Artif. Intell. Rev., doi: 10.1007/s10462-011-9276-0.

[7]. Rajabioun, R. 2011. Cuckoo optimization algorithm, Applied Soft. Computing, 11, 5508–5518.

[8]. Valian, E., Mohanna, S & Tavakoli, S. 2011. Improved cuckoo search algorithm for feed forward neural network training. International Journal of Artificial Intelligence Applications. 2(3): 36-43.

[9]. Brown, C., Liebovitch, L.S., Glendon, R. 2007. Lévy flights in Dobe Ju/hoansi foraging patterns, Human Ecol.35: 129-138.

[10]. Pavlyukevich, I. 2007. L´evy flights, non-local search and simulated annealing, J. Computational Physics, 226: 1830-1844.

[11]. Pavlyukevich, I. 2007. Cooling down L´evy flights, J. Phys. A: Math. Theor., 40: 12299-12313.

[12]. Reynolds, A. M. and Frye, M. A. 2007. Free-flight odor tracking in Drosophila is consistent with an optimal intermittent scale-free search, Plos One, 2: e354.

[13]. Yang, X.S.2010. Nature-Inspired Metaheuristic Algorithms. 2nd ed. United Kingdom: Luniver Press.

