M.KH. JASSIM

Petroleum Technology Department, University of Technology, Baghdad, Iraq

munag.nfama@gmail.com

Received on: 09/11/2016
Accepted on: 20/07/2017

Improved PSO Algorithm to Attack Transposition Cipher

Abstract- *Cryptanalysis is a complex and mathematically challenging field of study. It takes some data or message, which is called cipher text and attempt to restore its plaintext. This paper attempts to use an improved particle swarm optimization (PSO) to obtain the plaintext from the transposition cipher. This improved method gives a good performance for the PSO algorithm by generating best solution from the best to avoid stability to reach to solution (key). This key is used for breaking transposition cipher.*

Keywords- *Cryptanalysis, Modified PSO, PSO, Transposition cipher.*

How to cite this article: M.KH. JASSIM, “Improved PSO Algorithm to Attack Transposition Cipher,” *Engineering and Technology Journal*, Vol. 35, Part B, No. 2, pp. 144-149, 2017.

1. Introduction

Transposition cipher is a method of encryption of plaintext to produce a cipher. This method is based on rearrange the positions of plaintext according to some system. Therefore, the cipher text will be permutation of plaintext. The study of restore the message from cipher text to plaintext is known as cryptanalysis [1].

Many ciphers can be cryptanalyzed and broken in many ways. Some years ago, many of researchers which working in cryptography and cryptanalysis of ciphers are interested in the field of attacking transposition ciphers [2].

There are many methods applied on a large number of probable solutions to reach the one, which represent the desired solution. In this research, we attempt to use an improved PSO method to attach a transposition cipher. Particle swarm optimization (PSO) is a method depends on a population algorithm using the development of computers for solving such problems. It is based on the swarm intelligence that is based on social population principles to provide a possible solution [3]. PSO is method for the automatic recovery of the secret key, and then recover the plaintext from only the cipher text, using a mathematical model of the social interactions of swarms. This PSO algorithm gives us a good chance to obtain good solutions [4].

The proposed method is applied the attack on transposition cipher by improvement PSO, and this can be achieved by updating the new best solution from the previous best solution. The new iteration based on last iteration by taking a random subset of particles to improve the best solution. This technique is proposed to be more effective and give original PSO more energy by minimizing time to reach to the solution.

This research is organized as follow. Section 1 gave a brief introduction. The related work introduce in section 2. Section 3 and 4 introduce a brief discussion in transposition cipher and PSO algorithm respectively. The proposed improved method, experimental and results was discuses in details in section 5, 6. Conclusions in last section.

2. Related work

In the field of computational problems, it is sometimes more convenient to use an artificial intelligence with promising research opportunities and appreciable results. The first idea behind swarm intelligence was put by Millons in 1994, and then use the common behavior exhibited by the various swarm like bee colonies, fish schools, particle swarms, cuckoo birds. From these behaviors, the researchers can drawing a mathematical formulations and built a meta-heuristic algorithms like Ant Colony Optimization (ACO), Cuckoo Search Algorithm (CSA), Particle Swarm Optimization (PSO), Bee Colony optimization, and so on.

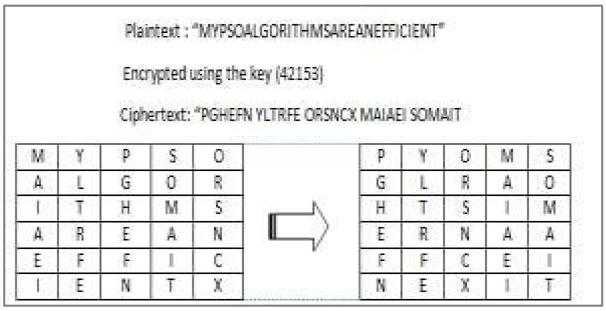
Meta-heuristic algorithms (Yang and Deb, 2010) are general-purpose search algorithms that be used to search of optimal or high quality solutions to a specific problem [5]. Danziger and Henriques (2011) are using the concept of swarm intelligence algorithms that can be applied to the field of cryptography [6]. Khan et al. (2013) propose a novel swarm based attack called Ant Colony Optimization to the cryptanalysis of Data

https://doi.org/10.30684/etj.2017.138650
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Encryption Standard (DES) [7]. Yang and Deb proposed a new algorithm called Cuckoo Search (Tuba, 2013), this approach was mathematical sound with a great amount of randomness which makes it quite ideal to be used in the field of cryptography as randomness provides strength to the code thus increasing the security [8]. Dr. Hilal H., Dr. Ahmed T., and Ismail K. used improved PSO to attack substitution cipher [9]. PSO is originally attributed to Kennedy, J., Eberhart, R. (1995). PSO can make a solution from few or no assumptions about the problem and then can optimized the solution by searching a very large space of candidate solutions. This method works iteratively trying to improve this candidate solution until reach the best one, which represent the best solution [10].

3. Transposition Ciphers

A simple transposition cipher is applied to a plaintext message by breaking this message into a fixed size of blocks and used a fixed size of permutation key P. The characters of each block will change its positions according to that key P. So the transposition cipher will has all its characters of its plaintext message. The decryption of the cipher text can be achieved by using same process of encryption but in the inverse permutation. A simple transposition cipher method is as the following example which change the order of words and also change the letters of each word, “a simple example” become “elpmaxe elpmis a”. Another method of transposition cipher is that change the order of the letters of each word but not change the order of the words, like the following example: “a simple example” will change to “a elpmis elpmaxe” [11]. Figure 1 give another example for transposition cipher.



Plaintext : “MYPSOALGORITHMSAREANEFFICIENT”

Encrypted using the key (42153)

Ciphertext: “PGHEFN YLTRFE ORSNCX MAIAEI SOMAIT

M	Y	P	S	O
A	L	G	O	R
I	T	H	M	S
A	R	E	A	N
E	F	F	I	C
I	E	N	T	X

P	Y	O	M	S
G	L	R	A	O
H	T	S	I	M
E	R	N	A	A
F	F	C	E	I
N	E	X	I	T

Figure 1: An Example for Transportation Cryptography [12]

Many researchers have studied breaking transposition cipher. Many researches in cryptanalysis on transposition cipher genetic algorithms, others used simulated annealing [2]. This research is applied improved PSO algorithm to attack transposition cipher.

4. Particle Swarm Optimization (PSO) method

PSO is a stochastic optimization technique developed by James Kennedy and Russell Eberhart in 1995. Particle swarm optimization has roots in two main component approaches. Its ties to artificial life (A-life) in general, and to bird flocking, fish schooling, and swarming theory in particular, and it is also related to evolutionary computation [1٠].

In usual, swam of birds while flocking and searching for food are either scattered or go together and searching until finding food. There is a strategy in finding the food that is always a bird is possible in the place when the food can be found. This bird represent the better food resource information, and this information will be transmitted at any time to others birds, the birds at end will be flock to the place where they can find the food. From this behavior and intelligent work, the particle swarm optimization algorithm is found. Because this technique is simple and easy to implement, this will give the PSO algorithm the way to use in many fields such us function optimization, the model classification, machine study, neutral network training, the signal procession, etc. [1٣].

I. The Principles of PSO:

PSO algorithm is starting with a random set of solutions called population, and then search with these solutions to find the best one by updating generations. In PSO, these random solutions called particles (birds). The particles are flying in the problem space, and following the best particle (best solution). PSO simulates the behavior of bird flocking. Suppose a group of birds searching randomly for food and they don’t know anything about the place where the food is found. The most proper strategy will be worked, the bird which is nearest to the food will be followed. In PSO, the birds represent the particles. Each one of these particles has its own fitness value which obtained from the fitness function, and has its velocity which direct the flying for these particles in the population in each generation. In each generation, there are two best values represent the best solutions. The first best solution is the fitness for each particle in the population, and this called ibest. The second one is the global best solution which is called gbest. This gbest is representing the best solution from the best solutions for all particles, and will obtain by any particle in the population. The optimizer of the swarm will track this gbest solution. Now, after finding the two best solutions, each particle will update its position and velocity using equations 1&2. [10]:

$$Vi[t+1] = wVi[t] + C1 * r1 * (Pibest[t] - Xi[t]) + C2 * r2 * (Pgbest[t] - Xi[t])$$

(1)

$$Xi[t+1] = Xi[t] + Vi[t+1]$$

(2)

Where: i =1,2,…..,N

w = the inertia weight, used to control the previous velocity vector of the particles on the new velocity vector. For better performance use range [0.8, 1.2] for w.

V[t] = the particle's velocity

X[t] = the current particle (solution)

ibest and gbest = the best solutions

r1 and r2 = two random numbers between (0,1). They are used to maintaining the variety of the population in equations 1 and 2.

C1 and C2 = learning factors, the default values=2.

Vmax = -Vmax represents lower range of velocity, Vmax represents upper range of velocity.

The basic algorithm for the PSO will be summarized as follow: [10]

1. Initialize the swarm:

X_i is the position of particles are randomly initialized within the hypercube of feasible space.

2. Evaluate the performance F of each particle, using its current position $X_i(t)$.

3. Compare the performance of each individual particle to its best performance:

IF $F(X_i (t)) < F(P_{ibest})$:
$F(P_{ibest}) = F(X_i(t))$
$P_{ibest} = X_i(t)$

4. Compare the performance of each particle to the global best particle:

IF $F(X_i(t)) < F(P_{gbest})$:
$F(P_{gbest}) = F(X_i(t))$
$P_{gbest} = X_i(t)$

5. Calculate the velocity of each particle according to equation (1).

6. Each particle will be moved to a new position using equation (2).

7. Go to step 2, and repeated until the rapprochement.

After each iteration, all particles positions will be updated for better position (Pibest). PSO algorithm is based on the social interaction. This is mean, each particle in the swarm will be learned from the other particles to obtain better knowledge which this particle move to best position that obtained previously for it and for his neighbors. Now, after each particle has its new best position, the Pgbest will be updated to the new best position within the completely new positions for all the swarm. This strategy depends on the communications between each particle with the other neighbors. This knowledge give each particle a way to imitates to go ahead to the best particle has the best position (best solution) [١٤, ١٥].

II. Cryptanalysis transposition cipher with PSO

PSO has been used in both continuous problems, and discrete space with transposition cipher. Figure 2 below shows using PSO attacking transposition cipher.

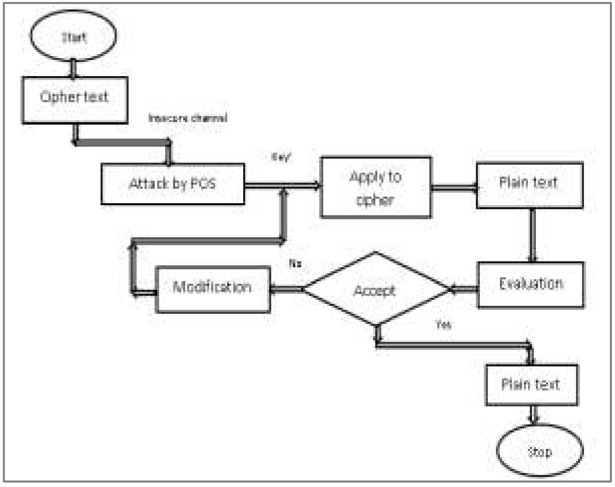


Figure 2: Transposition Cipher and Cryptanalysis using PSO

PSO is applying to simple transposition ciphers. PSO is searching for the key through the space of the cipher until reach the key and then decrypt cipher to obtain the plaintext.

The algorithm of transposition cipher use the following two steps:

1- The plaintext is written into rows and columns. Row wide is from 1 to N characters. Columns long is form from L MOD N characters. L is represent the long of the plaintext, and N is represent the long of the key.

2- The plaintext is arranged in rows beneath the key. Now start encrypt the plaintext in each row according to the key.

To cracking transposition cipher, first need to construct a population of particles, which is constructed randomly, then each particle represents an integer value assigned randomly. For example, suppose the key length is five, and then each particle has random value in range [0,120]. This range value converts to an integer permutation. For the beginning, the PSO algorithm starts with a population of values randomly generated between minimum and maximum operating limits of the generators and then assigned randomly to the particles. [3]

Table 1: Mapping between Integers and Integer Permutations

Practical i	Permutation key
0	04321
1	04312
2	04123
:	:
117	43012
118	43201
119	43210

To evaluate the particles, need to use a fitness function, which is represent in equation (3). Find the fitness value for all particles and set them as best value values for each one. The fitness function used with transposition cryptanalysis as follows:

$$Fitness = \sum_{i=1}^{29} \frac{frq[Di]}{L-1} + \sum_{j=1}^{12} \frac{frq[Tj]}{L-2} \quad (3)$$

Where:

frq[D_i] represent bigram letters frequency. Ex: (TH, AN, ON…)

frq[T_j] represent trigram letters frequency. Ex: (THE, AND, FOR…)

L is the text length

The fitness rating helps transposition cryptanalysis algorithm to reach to break the cipher. Depending on the scores to the number of times that two or three letters in English language commonly found and this will found actually in decrypted text. Then, the algorithm chose more columns to put to each other to achieve text that is more correct. When these combinations are achieved in decrypted text will give a higher value, which means that two or three columns suggested have been correctly aligned. As shown in following table (2). [1٦]

5. Proposed improvement of PSO:

The PSO algorithm description used to attack transposition cipher that proposed new idea is given bellow:

1- Give the cipher text, the length of it, and key permutation size. The score table such as the one in table (1).

2- Initializing the following algorithm parameters:

C_1 : Self-confidence

C_2 : Swarm confidence

W : Inertia weight

V_{max} : Max velocity

Swarm size : No. of particles in the swarm

Max-Iter : Max no. of iterations

3- Generate the initial particles randomly to form he swarm (keys of the simple transposition cipher).

4- For i=1, Max-Iter

a. For each particle (key) find the fitness function value by using equation (3).

b. If the current position of the particle is better than the previous one, update the particle's position with the better.

c. Find the best particle's position (key) from the better particles' positions of the swarm, and then update their positions using equation (3).

d. If there is no improvement in the better solution (key), then generate neighbor solution from the current best.

Table 2: 29 Diagram and 12 Trigram English letters combinations

29 Diagram Letters				12 Trigram Letters	
Diagram	**Percent**	**Diagram**	**Percent**	**Trigram**	**Percent**
TH	0.0250791	EA	0.0079078	ARE	0.0006778
HE	0.0237235	NG	0.0103931	THE	0.0153638
IN	0.0171713	AS	0.0112969	ING	0.0085856
RE	0.0115228	TI	0.0092634	ENT	0.0042928
AN	0.0153638	OR	0.0117488	AND	0.0085856
ED	0.0092634	IS	0.0092634	THA	0.0033891
ON	0.0108450	ET	0.0067781	NTH	0.0027113
ES	0.0131044	IT	0.0040669	WAS	0.0045188
ST	0.0151378	AR	0.0056484	HER	0.0011297
EN	0.0108450	TE	0.0070041	ETH	0.0038409
AT	0.0131044	SE	0.0079078	FOR	0.0020334
TO	0.0101672	HI	0.0063263	DTH	0.0009038
NT	0.0099413	OF	0.0074559	--------	---------
ND	0.0122006	HA	0.0079078	--------	---------
OU	0.0112969	---------	----------	---------	----------
Di-Total		Percent = 0.3246724		Tri-Total	0.0564844

Total	Percent = 0.3811568 = fitness of plaintext

5- The best solution (particle) will be copied as output solution, which represent the key and then exit.

After a new solution is made, it must be decided to make this new solution as a new generation or not. To accept the new solution as best solution, must new one give more performance from the previous best solution. But this may be lead us in a problem of no new best solution for a while and this will slow PSO method to reach to the solution (key). So, a new mechanism is used in proposed PSO to overcome this problem which is generate neighbor solution from the current best solution; this will give ability to generate new population of particles which can use it in next iterations to find the new best solution. This will precede to make new best solution and give us a good chance to improve the performance of the PSO algorithm.

The classic PSO is running much more time until reach to the result (key), because its check all the entire list of neighbors before make the decision to swap the best solution with the new best solution, whereas the improved PSO performs the swap after generate a new neighbor solution even when here is no improvement in solution.

6. Discussion and Experimental Results

In this paper, the basic or classical PSO and improved PSO used to attach simple transposition cipher. These two algorithms are used to cryptanalysis of simple transposition. The results will be summarized for these experiments in this section.

First comparison shows the performance of both PSO and Improved PSO. This comparison give more percentage of successful results for attacking transposition cipher by using Improved PSO.

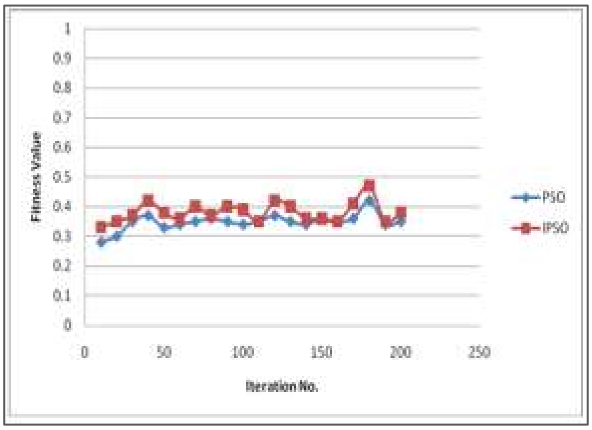


Figure 3: Performance of PSO and IPOS

Second comparison is made for classical transposition ciphers is based on the amount of ciphers to be attacked. The results of comparisons for different amount of cipher text are been arranged in Table 3. The key used in this table is in size of 15 elements, and the table gives the average number of key elements correctly discover by using both basic PSO and improved PSO techniques.

Table 3: The amount of key recaptured vs available ciphertext, Transposition cipher with size 15 using PSO and IPSO techniques

Amount of Ciphertext	Amount of key recovered (PSO)	Amount of key recovered (IPSO)
100	7.75	9.75
150	10	10
250	10.50	10.75
400	11.25	11.25
600	12	12.5
800	12.75	13
1000	13	13.25

The PSO returns the correct key or a candidate key that is close to the correct one. This means is still not the correct key, but can be used as a correct one especially when the transposition cipher is large. Even if there is some character not in its right place, the plaintext can be read.

In table 4: The comparison between PSO and IPSO according to the period used in transposition cipher. For period less than 15, both algorithms could successfully recover the key in most of the time. When the period become 20, the improved PSO is more powerful than basic PSO for recovering the key.

Table 4: The Amount of Key Recaptured Vs Transposition Size Using 1000 Known Ciphertext Characters

Transposition Size	PSO	IPSO
7	6.75	7
9	7.75	8
11	9	9
15	13	13.5
20	16.25	16.5
25	20	21.5

In table 5: shows the time in seconds, which required breaking the transposition, cipher of 1000 letters with different sizes of key.

Table 5: The Time Required to Break Transposition Cipher with 1000 Letters in size

Key Size	5	10	15	20	25
PSO Time (Sec.)	6	9	30	56	73
IPSO Time (Sec.)	7	10.5	32	58.5	76

7. Conclusion

This paper has argued that the PSO particle swarm optimization algorithm is a good way that can be used to cryptanalysis of ciphers, especially the transposition ciphers. In this work, the PSO algorithm clarifies that the transposition cipher can be broken. The improved PSO algorithm is implemented to cryptanalysis the transposition cipher that give a good performance to find results (keys), and dispose of the stability of the algorithm in some steps without change the results to reach the goal (key). The improvement will be in step without change the results (not gives best new solution), so this improvement give a great jump by generate a new best solutions from new swarm that give a good chance to change results. The new development got a percentage improvement in the number of detections keys ratio of nearly 9% better than the original method and the rate of increase in the time of 1.5 seconds.

References:

[1] C. Smith, "Basic Cryptanalysis Techniques", InfoSec Reading Room, SANS Institute 2001.

[2] A.T. Sadiq, L.A. Hashim, H. Kareem, "Attacking Transposition Cipher Using Improved Cuckoo Search", Journal of advanced computer science and technology, Vol. 4 (1), pp. 22-32, 2014.

[3] S.M. Hameed, D.N. Hmood, "Particles swarm optimization for the cryptanalysis of transposition cipher", Journal of Al-Nahrian university, Vol. 13 (4), December, pp.211-215, 2010.

[4] A.J. Clarks, "Optimization Heuristics for Cryptology", Queensland University of Technology, 1998.

[5] X.S. Yang and S. Deb, "Engineering optimization by cuckoo search", Int. J. Mathematical Modelling and Numerical Optimization, Vol. 1, No. 4, pp.330–343, 2010.

[6] M. Danziger, M.A.A. Henriques, "Computational Intelligence Applied on Cryptology: A Brief Review", CIBSI, Bucaramanga, Colombia, 2011.

[7] S. Khan, A. Ali and M.Y. Durrani, "Ant-Crypto, a Cryptographer for Data Encryption Standard", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[8] X.S. Yang, S. Deb, "Cuckoo search optimization metaheuristic adjustment", Recent Adv. Knowl. Eng. Syst. Sci., 2013.

[9] H. Salah ,A.T. Sadiq and Ismail K., "Attack on the Simple Substitution Ciphers Using Particle Swarm Optimization ", Eng. & Tech. Journal, Vol.28, No.11, 2010.

[10] J. Kennedy and R. Eberhart, "A New Optimizer Using Particle Swarm Theory", Purdue School of Engineering and Technology, 1995.

[11] D.R. Clark, "Simple Transposition Ciphers", Crypto Corner, crypto interactive math's , 2013

[12] G.J. Simmons , "Transposition cipher cryptology", Encyclopedia Britannica, School and Library Subscribers, 2016.

[13] Q. Bai, "Analysis of Particle Swarm Optimization Algorithm", Computer and Information Science, College of Computer Science and Technology, China, Vol. 3 (1), pp. 180-184, 2010.

[14] Y. Shi and R.C. Eberhart, "A Modified Particle Swarm Optimizer", Proc. IEEE Conference on Evolutionary Computation, IEEE Xplore digital library, pages 69-73, 1998.

[15] M.A. Khanesar, M. Teshnehlab, and M. A. Shoorehdeli, "A Novel Binary Particle Swarm Optimization", Proc. 15th Mediterranean Conference on Control and Automation, IEEE Xplore digital library, pp. 1-6, 2007.

[16] A.T. Sadiq, "Mutation-Based Particle Swarm (MPSO) to Attack Classical Cryptography Methods", Journal of Advanced Computer Science and Technology Research (2), pp. 50-65, 2012.

Author biography

M. KH. JASSIM, M.Sc. in Computer Science, University of Technology, Baghdad, Iraq. Her research interest are IPSO algorithm used to attack transposition cipher by finding the key using to break the cipher. M. KH. JASSIM is currently assistant lecturer in Petroleum Technology Department, University of Technology, Baghdad, Iraq.