International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 11 – No. 11, March 2017 – www.ijais.org

Cryptanalysis of Nonlinear Stream Cipher Cryptosystem based on Improved Particle Swarm Optimization

Salim A. Abbas Al-Ageelee, PhD
Dept.of ComputerScience &
Al-Mustansiriya University

Riyam N. J. Kadhum
Dept.of ComputerScience &
Al-Mustansiriya University

ABSTRACT
Stream cipher is one of the hard electronic cipher systems because of high security and difficulty in breaking it. In this paper the proposed cryptanalysis system based on a Particle Swarm Optimization (PSO) with suggestions for improving the achievement of PSO, by using Simulated Annealing (SA) that is the first part of this paper. The second part represented by a comparison study for the cryptanalysis results obtained by the Improved PSO (IPSO) with classical PSO and Genetic Algorithm (GA).The cryptanalysis process include finding the initial state of the attacked stream cipher cryptosystem using ciphertext only attack.

Keywords
Stream Cipher System, Cryptanalysis, Particle Swarm Optimization, Genetic Algorithms, Simulated Annealing, Improved Particle Swarm Optimization..

1. INTRODUCTION
Cryptanalysis is the science of recovering the plaintext of a message without access to the key. It is a method of transforming cipher text into a plaintext without knowing the key or algorithm [1].

However the cryptanalysis of stream ciphers through soft computing techniques as Particle Swarm Optimization (PSOs), Genetic Algorithms (GAs) is still an emerging issue. GA is based on the evolutionary ideas of Natural selection and genetics [2]. GA is a good condidate for the optimal solutions to optimization and search problems. The algorithm has been successfully applied to Vertex-Cover problem [3], Maximum-Clique problem [4], Regression testing [5], N-puzzle problem [6], Traveling Salesman Problem [7].

PSO was originally developed by a social-psychologist J. Kennedy and an electrical engineer R.Eberhart in 1995 and emerged from earlier experiments with algorithms that modeled the "flocking behavior" seen in many species of birds. Where birds are attracted to a roosting area in simulations they would begin by flying around with no particular destination and in spontaneously formed flocks until one of the birds flew over the roosting area [8]. PSO has been an increasingly hot topic in the area of computational intelligence. It is yet another optimization algorithm that falls under the soft computing umbrella that covers genetic and evolutionary computing algorithms as well [9]. There are many researches has been written on using soft computing techniques to cryptanalysis different types of encryption systems some of these: A.J.Clark, in his Thesis uses various optimization heuristics in the fields of automated cryptanalysis and automated cryptographic function generation[10], M.F. Uddin in his paper focused on using of PSO in cryptanalysis of simple substitution ciphers using ciphertext only attack[11], R.R.Yako In her research, an optimization approach such as GAs is considered to improve the cryptanalysis problem[12], S. M. Hameed in her work used PSO to cryptanalysis transposition cipher, PSO used ciphertext only attack to recover the secret [13], H.A.M Al_Sharifi,in his research focused on using of PSO algorithm to cryptanalysis stream cipher using plaintext attack choosing one Linear Feedback Shift Register (LFSR) [14], B.N. Ferriman, in his Thesis focused on the RC4 algorithm and present a new approach for cryptanalysis of the cipher by attacking RC4s state register[15], Ali A. Abd in his research is considered a new approach to cryptanalysis stream cipher systems based on GA [16]. The present work explores the related work done and applicability of GAs and PSOs in a field of cryptanalysis.

In this paper the proposed technique employed for the purpose of Cryptanalysis

To apply ciphertext only attack to cryptanalysis the Geffe system as a case study of stream cipher cryptosystem. This technique exploites hybridization between PSO and SA.

The rest of this paper has been organized as follows: Section 2 presents a brief overview of soft computing techniques. Section 3 presents designing cryptanalysis systems for stream cipher. Section 4 presents a comparison result of cryptanalysis system between GA, PSO and IPSO. The last section explains the conclusion.

2. SOFT COMPUTING TECHNIQUES
2.1 Genetic Algorithm
GAs is the search heuristic that mimics the process of natural evolution [2]. It is based on the Darwin's principle of Natural selection. According to this theory the chromosomes with the best fitness function should survive and create new offspring (survival of the fittest). GAs gives useful solution to optimization and search problem. It is a rapidly growing area of Artificial Intelligence. The GAs starts with the population which is nothing but chromosomes which can be decimal or binary or even hexadecimal. The GAs operator is applied to population in order to optimize the results [17]. The new population is formed from the old population with better fitness value. The population can be crafted using the operators: Population size, Fitness Function, Selection, Crossover, Mutation. [18, 19, 20].

2.2 Particle Swarm Optimization
Swarm Intelligent is a kind of Artificial Intelligence based on the behavior of animals living in groups and having some ability to interact with another and with the environment in which they are inserted. Every particle in the swarm acts in a distributed manner using the intelligence of its own and the group intelligence. Every particle has two features: a position and a velocity. The particles exchange the information to

correct their positions and velocities by using the received information [21].

2.2.1 Basic Elements of the PSO Technique [22,23].

The basic elements of PSO technique are briefly stated and defined as Follows:

1-Particle, X^i : It is a candidate solution represented by an m-dimensional vector, where m is the number of optimized parameters.
2- **Population, pop(t)** : It is a set of n particles at time i, i.e. pop(i) = $[X^i_1, ..., X^i_n]$T. The number of particles in population would be between 20 to 30.
3- **Swarm**: It is an unsystematic moving particles population, which Band together and at the same time every particle moves in a Unorganized direction.
4- **Particle velocity, V_i**: It is the speed of the moving particles which can be characterized by k-dimensional vector.
5- **Inertia weight, w_i** : It is a control factor used to control the effect of the preceding velocities on the present velocity.
6- **Individual best, p_i** : it is the composition of the particle fitness value at the present position to the best fitness value it has ever reached.
7-**Global best, p_j^g**: It is the best location obtained in all individual locations.
8-**Stopping criteria**: it is the terms which finish search process.

2.2.2 PSO Methods

There are several methods of PSO depending on the shape of Updated velocity equation of the particle those are:

Original PSO **:** Basic algorithm introduced to calculate the velocity and position of each particle and it is used to find the Optimal solution**.** velocity of individual particles updated as follows: $V^i_{j+1}=V^i_j+c_1r_1(P^i_j - X^i_j) +c_2r_2 (P^g_j- X^i_j)$ (1) j=1,…,n with the position calculated as follows: $X^i_{j+1}=X^i_j+V^i_{j+1}$ (2) j=1….,n

Where:

X^i_j : Particle position

V^i_j : Particle velocity

P^i_j: Best position found by jth particle

P^g_j: Best position found by swarm

c_1 and c_2 : are the cognitive (individual) and social, (group) learning, rates, respectively, The values of c_1 and c_2 are usually assumed to be 2.

r_1 and r_2 : are uniformly distributed random numbers in the range 0

and 1.

Inertia Weighted PSO **:** The inertia weighted PSO is added to decrease the velocity. Its value varies from 0.9 to 0.4. The value of the jth particle velocity can be formilated as:

$$V^j_{j+1} = w_i v_j^i + c_1 r_1 (p_j^i - x_j^i) + c_2 r_2 (p_j^g - x_j^i)$$

J=1,…,n (3)

Then the value of the inertia weight can be calculated :

$$w_i = W_{max} - (W_{max} - W_{min}/imax) * i \quad (4)$$

where:

W_{max} is the initial value of the weight.

W_{min} : is the final value of the inertia weight.

i_{max} : is the maximum number of iterations.

In this work, Inertia Weighted PSO type is used.

2.3 Simulated Annealing

Simulated annealing is based on the concept of annealing. In physics, the tern annealing describes the process of slowly cooling a heated metal in order to attain a "minimum energy state". A heated metal is said to be in a state of "high energy".. The technique merges hill-climbing with the probabilistic acceptance of non-improving moves. The search starts at some initial state S = S0. There is a control parameter T known as the temperature. This starts 'high' at T0 and is gradually lowered. At each temperature, a number of moves to new states are attempted. A candidate state is randomly selected from the neighborhood of the current state. The change in value of the cost function is calculated. If it improves the value of cost function, then a move to that state is taken; if not, then it is taken with some probability. Probabilistic acceptance is determined by generating a random value in the range (0, 1) and performing the indicated comparison. The algorithm is discussed below [24].

2.3.1 Basic Simulated Annealing

According to statistical thermodynamics, $P\alpha$, the probability of a physical system being in state α with energy $E\alpha$ at temperature T satisfies the Boltzmann distribution.
where kB is the Boltzmann's constant, T is the absolute temperature, and Z is the partition function, defined by:

$$P\alpha = 1/Z \; e^{(-E\alpha / k_B)^T} \quad (5)$$

$$Z=\sum_\beta e^{-(E_B /Kb)^T} \quad (6)$$

the summation being taken over all states β with energy $E\beta$ at temperature T. At high T , the Boltzmann distribution exhibits uniform preference for all the states, regardless of the energy. When T approaches zero, only the states with minimum energy have nonzero probability of occurrence. In SA, the constant kB is omitted. At high T , the system ignores small changes in the energy and approaches thermal equilibrium rapidly, that is, it performs a coarse search of the space of global states and finds a good minimum. As T is lowered, the system responds to small changes in the energy, and performs a fine search in the neighborhood of the already determined minimum and finds a better minimum. At T = 0, any change in the system states does not lead to an increase in the energy, and thus, the system must reach equilibrium if T = 0. When performing SA, theoretically a global minimum is guaranteed to be reached with high probability. The artificial thermal noise is gradually decreased in time. T is a control parameter called *computational temperature*, which controls the magnitude of the perturbations of the
energy function $E(x)$. The probability of a state change is determined by the Boltzmann distribution of the energy difference of the two states:

$$P = e^{-(\Delta E / T)} \quad (7)$$

The probability of uphill moves in the energy function ($\Delta E > 0$) is large at high T ,and is low at low T . SA allows uphill moves in a controlled fashion: It attempts to improve on greedy local search by occasionally taking a risk and

accepting a worse solution. The algorithm of simulated annealing as following:[24].

1. Initialize the system configuration.
   Randomize $\boldsymbol{x}$ (0).
2. Initialize T with a large value.
3. **Repeat**:
   a. **Repeat**:
   i. Apply random perturbations to the state
   $\boldsymbol{x} = \boldsymbol{x} + \Delta\boldsymbol{x}$.
   ii. Evaluate $\Delta E(\boldsymbol{x}) = E(\boldsymbol{x} + \Delta\boldsymbol{x}) - E(\boldsymbol{x})$:
   if $\Delta E(\boldsymbol{x}) < 0$, keep the new state;
   otherwise, accept the new state with probability $P = e^{-\Delta E/T}$.
   until the number of accepted transitions is below a threshold level.
   b. Set $T = T - \Delta T$.
   until T is small enough.

3. DESIGNING CRYPTANALYSIS SYSTEMS FOR STREAM CIPHER

In this work the soft computing techniques used as GA and PSO and proposed technique IPSO which could be implemented and applied easily to solve various optimization problems. These techniques employed for the purpose of Cryptanalysis. We suggest main steps to designing cryptanalysis systems for stream cipher, we select the Geffe generator to be attacked .these steps of the analysis and procedure can be summarized as follows:

Step1: select ciphertext (Ci).

Step2: generate the key stream (Ki) from Geffe generator system.

Step3: calculate the plainrtext(Pi) as follows:

Ci XOR Ki=Pi .

Step4: design fitness function depending on the probability of numbers of 0's in Pi

Step5: apply soft computing techniques.

Step6: repeat step2 until stopping criteria satisfied.

3.1 Fitness Function Calculation

The main goal of cryptanalysis is to get the key in order to obtain the plaintext. Cryptanalysis stream cipher should get the correct key to decrypt the ciphertext. Using soft computing techniques to cryptanalysis stream cipher needs fitness to determine the best new generation. In this work, new fitness function based on xoring between Cn and Kn. Cryptanalysis of stream cipher based on statistical model is used to find the Linear Feedback Shift Regester (LFSRi) part of the key, i.e., the initial of the LFSRi, i $\in$ {1, …, s}. Where:

C_n:cipher text digits.

K_n:the output key of Geffe generator

N: ciphertext length

Let n_0 be the number of 0's in P_i ,then:

Fitness = $P(0) = n_0 / N$ (8) Here, the best fitness >= 0.60, this rate considered the threshold in our work, it change according to different plaintext size.

We will attack the Geffe generator, nonlinear combining function which it consist of 3 LFSR in different Length:3,5,7.

The algebraic normal form is:

f (x1, x2, x3) = x1x2 XOR x2x3 XOR x3. (9)

Here, the number of ciphertext symbols is determined to perform a ciphertext-only attack on the Geffe Cipher using the correlation attack. Our conclusion from the analysis is that the pseudonoise generator's output sequence and the sequences generated by the linear feedback shift registers (LFSR) should be uncorrelated. This leads to constraints for the nonlinear combining function to be used.

3.2 Using Genetic Algorithm (GA) to cryptanalysis stream cipher systems

GA has been successfully applied to numerous applications in the field of search and optimization. It is recursive procedure that consists of a fixed population size of chromosomes. These chromosomes are created randomly or heuristically which represent the initial population. The population evolves by applying three basic operations: selection crossover and mutation with probability For the Initial Population, the cryptanalysis process begins with randomly generated numbers between {0, 1} as the key size for n chromosomes and sorting these numbers in ascending order. The sequence of these numbers represents the candidate keys (chromosomes). Each chromosome represents the candidate key which it uses to decrypt the ciphertext and then calculate the fitness value to determine the best chromosome (candidate key).

For the Selection operator, selects chromosomes in the population for reproduction. The better chromosome has the opportunity to select more timed to reproduce. Many selection procedures have been proposed, this paper used Roulette-wheel selection selection which is the better individuals will be chosen more often than the poorer ones, thus fulfilling the requirements of survival of the fittest [24]. to attack nonlinear stream cipher systems, which it used to selecting potentially useful solutions for reproduction. The chromosome (sequence) with high fitness has a higher probability of participate one or more offspring to the next generation. For the Crossover operator, two chromosomes are combining to produce a new generation that possesses both their characteristic. There are several crossover techniques, in this paper we will use single-point crossover which is One crossover point is selected, binary string from beginning of chromosome to the crossover point is copied from one parent, the rest is copied from the second parent [25]. with probability of crossover (pc) equal to 0.7 to attack stream cipher. For Mutation operator flips the bit in chromosomes. The purpose of mutation is to maintain the diversity within the population. in this paper we will use the Flip Mutation: Flip Mutation causes one bit to be randomly selected within the chromosome and then flipped, a 1 is changed to a 0 and a 0 is changed to a 1. The Probability of mutation (pm) equal to 0.1. For the Fitness Function calculation in this paper, equation (8) is used to calculate the fitness function of GA to attacks stream cipher. For the GA parameters there are a set of values which are considered as the most appropriate to attacks stream cipher by GA different parameters of GA to cryptanalysis stream cipher Systems (see Table 1).

3.3 Using PSO algorithm to cryptanalysis stream Cipher

In Evaluation For the initial population, the cryptanalysis process begins with randomly generated numbers between {-1, 1} as the key size for n particles .The sequence of these numbers represents the candidate keys (particles). Randomly generates Velocity for each particle which it's bounded to some minimum and maximum values [Vmax, Vmin] where Vmin= -Vmax and it uses to reinforces the local search reconnoitering of the problem space. Each particle represents the candidate key and use to decrypt the ciphertext and then calculate the fitness value to determine the best particle (key). For the evaluation process, the fitness value for each particle (candidate key) must be calculated for each generation. Table 2 shows the most parameters of PSO that preferred to be used to decrypt stream cipher.

3.4 Using IPSO algorithm to cryptanalysis stream Cipher

In IPSO the proposed cryptanalysis system used to apply ciphertext only attack to cryptanalysis the Geffe system using soft computing techniques exploded a hybridization between PSO and Simulated Annealing (SA).(see Fig.1) shows the Flow Chart of proposed system . In IPSO we will use the same parameters of classical PSO as mentioned in Table 2. The following Table 3 shows the parameters used in IPSO.

4. COMPARISON RESULTS OF CRYPTANALYSIS SYSTEM BETWEEN GA, PSO AND IPSO.

The following Tables 4,5, and 6 shows the results of applying proposed cryptanalysis system GA , PSO and IPSO For Popsize(20,100,200) and Maxiter(100,300) For TxtLen=100,40,10 characters ,The following notations are used:

Popsize = Population size.

MaxIter= Maximum Iteration.

BF=Best Fitness.

T/sec=Time/second.

T.T/sec=Total Time/second.

Iter_Num= Iteration_Number.

Fig. 2 shows the comparison between GA , PSO and IPSO in cryptanalysis system for Popsize =100 and MaxIter=100 for TxtLen=100 (see Figure 2).

Table 5 shows the results of GA For Popsize(20,100,200) and Maxiter (100,300) For TxtLen=40 characters.(see Table 5).

Fig. 3 Shows the comparison between GA, PSO and IPSO in cryptanalysis system for Popsize =200 and MaxIter=100 for TxtLen=40 (see Fig. 3).

Table 6 shows the results of GA,PSO and IPSO For Popsize(20,100,200) and Maxiter(100,300) For TxtLen=10 characters (see Table 6).

Fig. 4 Shows the comparison between GA, PSO and IPSO in cryptanalysis system for Popsize =20and MaxIter=300 for TxtLen=10.

(see Fig. 4).

Table 1 : GA parameters to attack stream cipher.

Parameters	Symbol	Value
Key Length	KeyLen	[12]
Text Length	TxtLen	[10-100]
Number of chromosomes	Popsize	[20,100,200]
Maximum number of Iteration	MaxIter	[100-300]
Probability of crossover	P_c	0.7
Probability of mutation	P_m	0.1

Table 2 : PSO parameters to attack stream cipher.

Parameters	Symbol	Value
Number of particles in the swarm	Popsize	[20-200]
Number of Key	KeyLen	[12]

Length of text	TxtLen	[10-100]
The maximum number of Iteration	MaxIter	[100-300]
The maximum of velocity	V_{max}	4
The minimum of velocity	V_{min}	$-V_{max}$
Inertia Weight	W	[0.4-0.9]
Acceleration parameter	C_1,C_2	[0.5-2]
Random number between [0,1]	r_1,r_2	[0-1]

Table 3: IPSO parameters to attack stream cipher

Parameters	Symbol	Value
Number of particles in the swarm	Popsize	[20-200]
Number of Key	KeyLen	[12]
Length of text	TxtLen	[10-100]
The maximum number of Iteration	MaxIter	[100-300]
The maximum of velocity	V_{max}	4
The minimum of velocity	V_{min}	$-V_{max}$
Inertia Weight	W	[0.4- 0.9]
Acceleration parameter	C_1,C_2	[0.5-2]
Random number between [0,1]	r_1,r_2	[0-1]
Initial temperature	T	0.1

Table 4: results of applying GA , PSO and IPSO for Popsize(20,100,200) and MaxIter(100,300) for TxtLen=100 characters.

Popsize	MaxIter	GA				PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num
20	100	0.5869	2.09	15.91	13	0.6188	0.23	16.31	1	0.5657	0.35	14.70	1
	300	0.5496	0.67	48.30	4	0.5520	0.58	47.20	1	0.5682	0.32	43.39	1
100	100	0.6301	3.21	79.33	3	0.5656	1.21	82.32	2	0.6301	1.43	72.55	1
	300	0.6023	4.84	238.36	6	0.5556	0.82	240.98	1	0.5669	1.45	215.47	1

200	100	0.6048	4.86	163.88	3	0.5850	3.29	160.47	2	0.5769	2.89	144.13	1
	300	0.5694	5.62	476.26	4	0.5760	1.58	460.32	1	0.5807	2.80	423.01	1

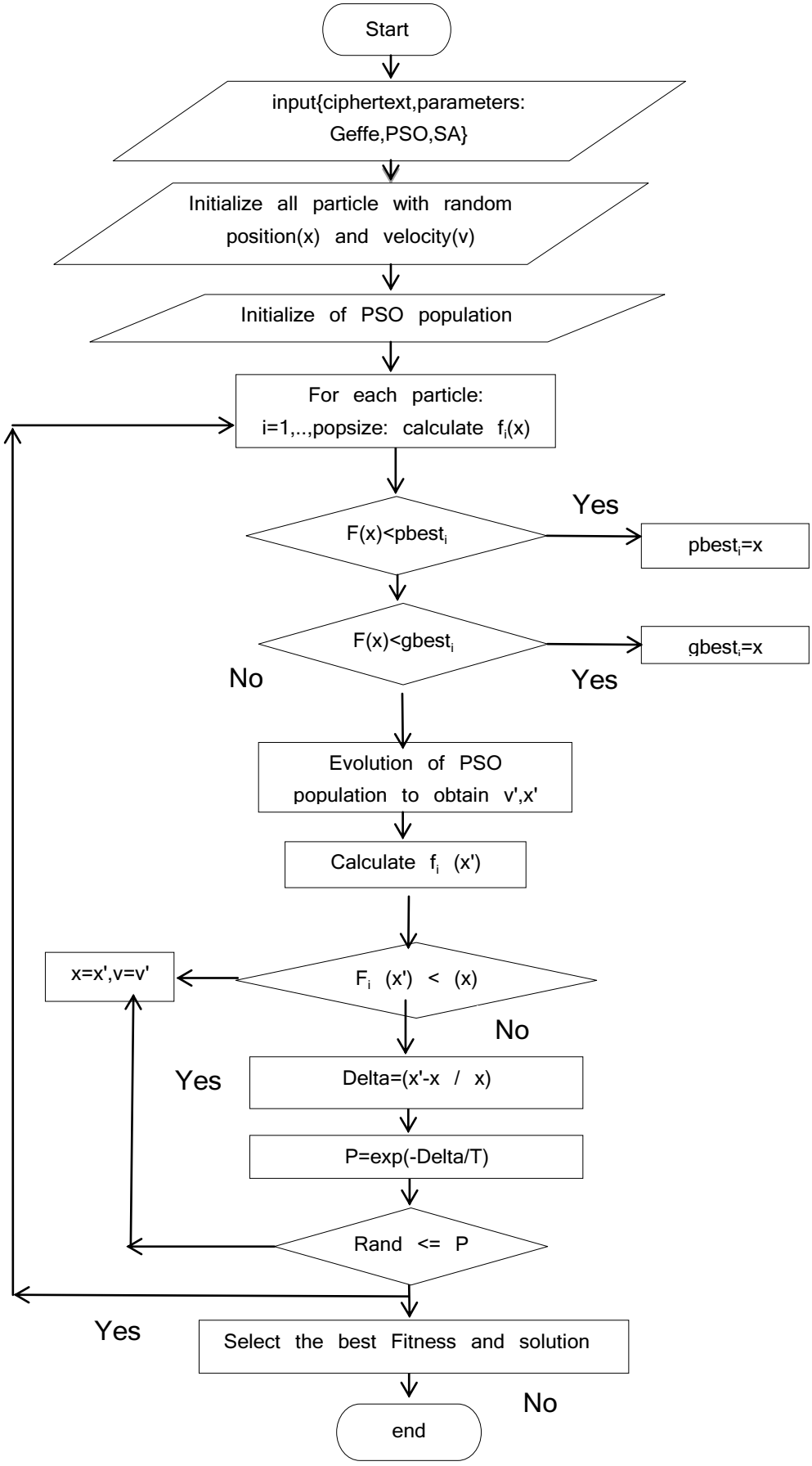
Table 5: results of applying GA, PSO and IPSO for Popsize(20,100,200) and MaxIter(100) for TxtLen=40 characters.

Popsize	MaxIter	GA				PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num
20	100	0.5906	2.11	6.98	31	0.5656	0.17	6.97	2	0.5563	0.14	6.69	1
	300	0.5938	0.21	19.81	3	0.5875	0.18	22.41	2	0.5656	0.22	19.96	1
100	100	0.5625	25.48	33.99	75	0.6188	0.70	32.75	2	0.5750	0.65	32.56	1
	300	0.6262	20.30	101.30	35	0.6262	0.41	97.51	1	0.5500	0.55	98.70	1
200	100	0.6094	30.10	65.50	35	0.6125	0.66	64.53	2	0.6188	0.22	64.46	1
	300	0.6023	5.60	465.30	4	0.5906	1.60	463.10	1	0.5800	0.56	192.10	1

Table 6: results of applying GA, PSO andIPSO for Popsize (20,100,200) and MaxIter (100,300) for TxtLen=10 characters.

Popsize	MaxIter	GA				PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter-Num	BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter-Num
20	100	0.6250	0.11	2.02	5	0.6250	0.05	2.10	1	0.6062	0.03	1.75	1
	300	0.6750	0.83	5.87	42	0.6625	0.04	5.60	2	0.6250	0.05	6.15	1
100	100	0.6250	1.96	10.99	18	0.6625	0.09	8.50	1	0.6375	0.22	9.19	1
	300	0.6625	27.25	33.36	250	0.6625	0.81	24.40	1	0.6250	0.22	26.10	1
	100	0.6750	12.25	27.34	45	0.6625	0.18	16.80	2	0.6375	0.36	17.51	1

200	300	0.6625	13.92	82.10	51	0.6625	0.35	50.47	2	0.6500	0.38	51.93	1


Start
input{ciphertext,parameters: Geffe,PSO,SA}
Initialize all particle with random position(x) and velocity(v)
Initialize of PSO population
For each particle: i=1,..,popsize: calculate $f_i(x)$
$F(x)<pbest_i$
Yes
$pbest_i=x$
$F(x)<gbest_i$
No
Yes
$gbest_i=x$
Evolution of PSO population to obtain v',x'
Calculate f_i (x')
F_i (x') < (x)
x=x',v=v'
No
Yes
Delta=(x'-x / x)
P=exp(-Delta/T)
Rand <= P
Yes
Select the best Fitness and solution
No
end

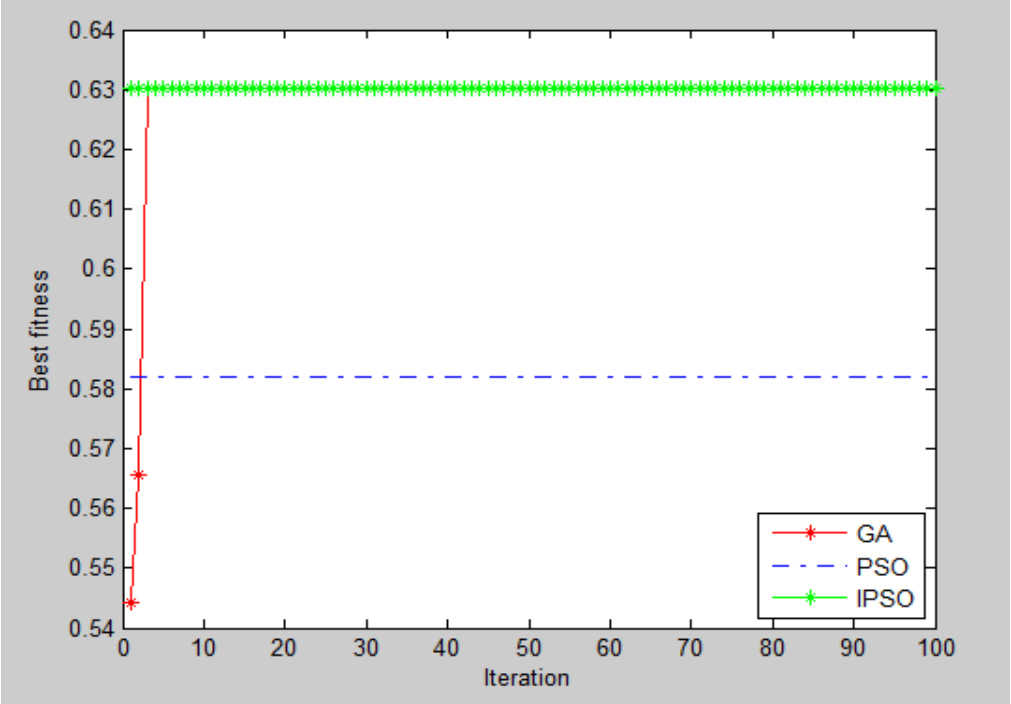


Fig. 2 Comparison between GA, PSO and IPSO in cryptanalysis system for Popsize =100 and MaxIter=100 for TxtLen=100.

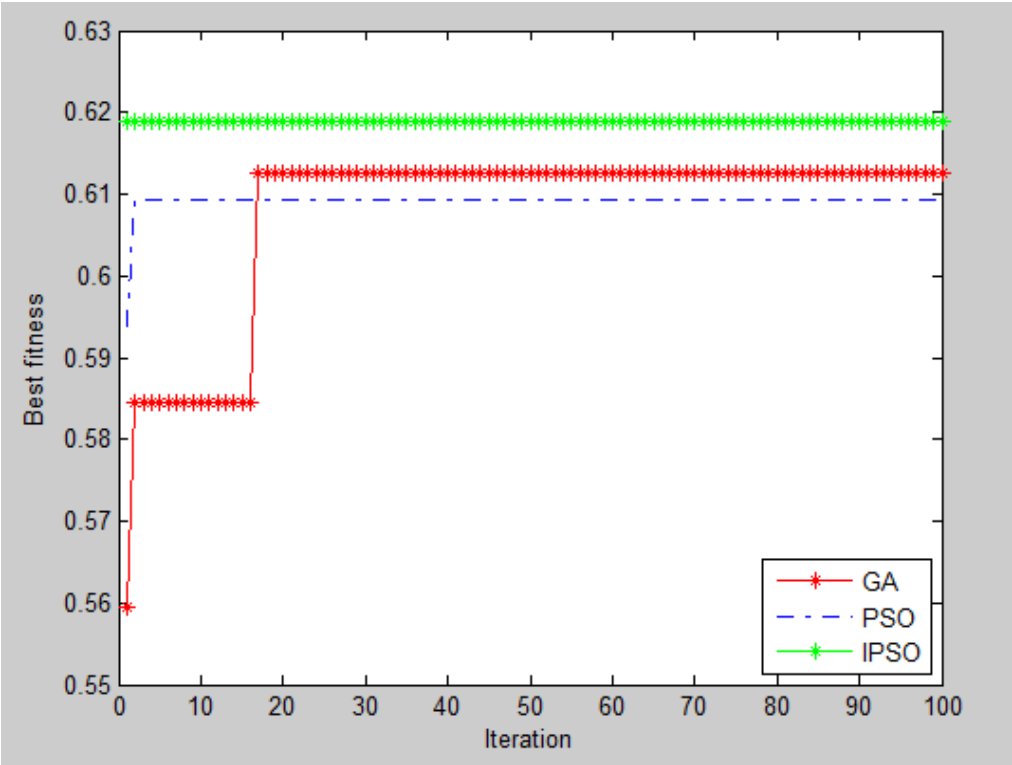


Fig. 3 Comparison between GA, PSO and IPSO in cryptanalysis system for Popsize =200= and MaxIter=100 for TxtLen=40.

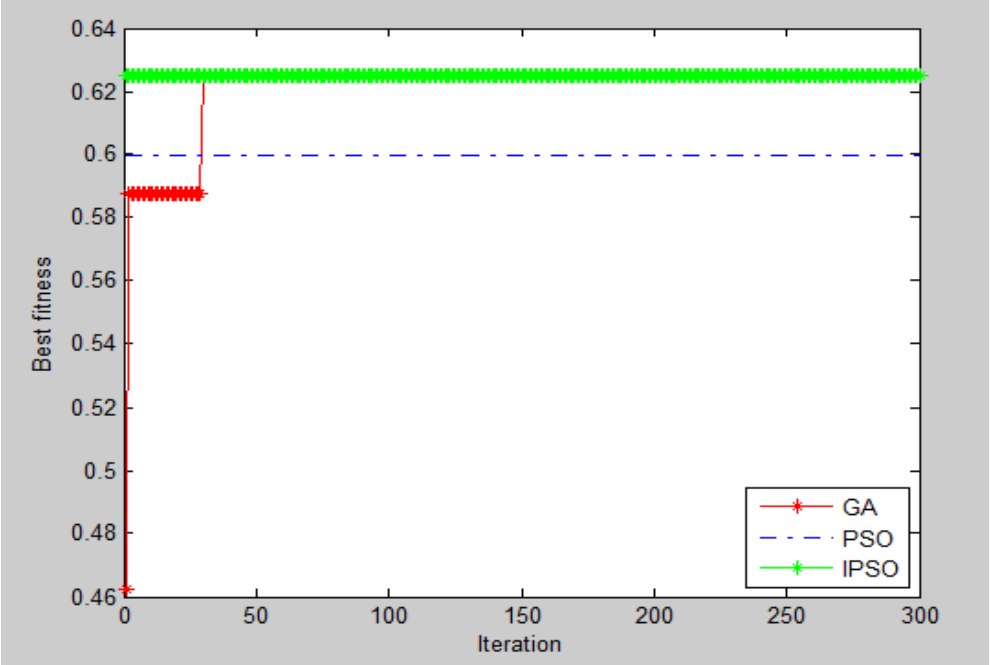


Fig.4 Comparison between GA, PSO and IPSO in cryptanalysis system for Popsize =20 and MaxIter=100 for TxtLen=10.

5. CONCLUSIONS

1-The cryptanalysis system using GA, PSO and IPSO can find the optimal solution for text till lengths with 10 characters as shown in Tables 6.

2-As shown in Tables 4, 5 and 6 the results of applying GA, PSO and IPSO to cryptanalysis stream cipher, we notice that 3 iterations are enough to find the best solution for the PSO and IPSO but this number of iterations are not enough for GA to find the best solution.

3-The performance of GA is less than the performance of the other two techniques in cryptanalysis stream cipher in the term time as shown in Tables 4, 5 and 6.

4-As shown in Table 4 we conclude that the best results of GA, PSO and IPSO in TxtLen=100 characters are obtained in Popsize=100 and MaxIter=100.

5-As shown in Table 5 the best results of GA, PSO and IPSO in TxtLen=40 characters are obtained in Popsize=200 and MaxIter=100.

6-As shown in Table 6 we conclude that the best results of GA , PSO and IPSO in TxtLen=10 characters are obtained in Popsize=20 and MaxIter=100.

7-From a sequent 4,5 and 6 ,we conclude that Popsize=200 and MaxIter=100 is enough to find the optimal key for the three techniques.

8-The time consuming in cryptanalysis of stream cipher systems based on GA and PSO are less than IPSO for most cases.

6. REFERENCES

[1] Schneier, B.1996, Applied Cryptography, Second Edition: Protocols, Algorithms andSource Code in C.

[2] Holland,J.H.1992,Adaptation in Natural andArtificial Systems.

[3] M.Milanovic,"Solving the generalised vertexcover problem by Genetic Algorithm ", Computing and Informatics,2010.

[4] Bazgan,C.,Luchian,H.1995. A geneticAlgorithm for maximal Clique Problem. Inproceeding of the International Conference in Ales,France.

[5] H.Bhasin,Manoj,"Regression testing using Coupling and Genetic Algorithms", InternationalJournal of Computer Science and Information Technologies,2012.

[6] H.Bhasin,N.Singla,"Genetic based algorithm forN-Puzzle problem", International Journal of Computer Application,2012.

[7] Y.Liao et al,"Evolutionary algorithm toTraveling Salesman Problems", Computer &Mathematics with Applications,2012.

[8] Papoulis, A. "Probability Random Variables,and Stochastic Process", McGraw-Hill College,October, 2001.

[9] Parsopoulos K. E. and Vrahatis M.N., "Recent Approaches to Global optimization Problemsthrough Particle SwarmOptimization", Kluwer Academic Publishers, Netherlands, Natural Computing 1, pp 235–306, 2002.

[10] A.J.Clark," Optimisation Heuristics for Cryptology", Information Security ResearchCentre Faculty of Information TechnologyQueensland University of Technology, 1998.

[11] M. F Uddin and Amr M. Youssef," Cryptanalysis of Simple Substitution Ciphers Using Particle Swarm Optimization". IEEE,Congress on Evolutionary Computation,Canada,2006.

[12] Rajaa R.Yako," Decrypting A Class Of Stream Cipher Using Ciphertext Only, ComparativeStudy", Master Thesis, Higher Academy for Scientific and Humanistic Studies, Departmentof Computer Science,2007.

[13] Sarab M. Hameed and Dalal N. Hmood, "particles swarm optimization for the cryptanalysis of transposition cipher " . Journalof Al-Nahrain University , Vol.13(4),pp.211-215, 2010.

[14] Hussein Ali Mohammed Al_Sharifi ," Cryptanalysis of Stream Cipher System Using Particle Swarm Optimization Algorithm ".Journal of Kerbala University , Vol. 8 No.4 Scientific , 2010.

[15] Benjamin Nicholas Ferriman," Cryptanalysis of the RC4 Stream Cipher using EvolutionaryComputation Methods",Master Thesis, University of Guelph, Guelph, Canada,2013.

[16] Ali A. Abd , Hameed A. Younis, and Wasan S.Awad," Attacking of stream Cipher Systems Using a Genetic Algorithm". Journal of Univesity of Thi-Qar, ISSN: 66291818,Vol. 8, Issue. 3, 2013.

[17] Goldberg,D.E.1989. Genetic Algorithm insearch, optimization and machine learning.

[18] Goldberg,D.E et al.2000. BayesuanOptimization Algorithm, population sizing and time to convergence, University of Illinois,USA.

[19] Melanie,M.1996. An introduction to a GeneticAlgorithm:MIT press paperback edition.

[20] Bhasin,H.2015.Algorithms: Design andAnalaysis.

[21] Singiresu S. Rao "Engineering Optimization Theory and Practice" Book, by John Wiley & Sons, Inc.2009.

[22] James Kennedy and Russell Eberhart "Particle Swarm Optimization", Book, IEEE 1995.

[23] James Kennedy "The Particle Swarm: Social Adaptation of Knowledge" IEEE, 1997.

[24] S. C. Krirkpatrick, J. D. Gellatt, and M. P. Vecchi, “Optimization by simulated annealing”, Science, vol. 220,no.4598,pp.671-680,1983