ISSN: 0067-2904

Secure Big Data Transmission based on Modified Reverse Encryption and Genetic Algorithm

Methaq Talib Gaata[1*], Zied O. Ahmed[1], Rasha S. Ali[2]
[1]*Computer Science Department, College of Science, Mustansiriyah University, Baghdad, Iraq*
[2]*Electrical Engineering Department, College of Engineering, Al Iraqia University, Baghdad, Iraq*

Received: 30/1/2022 Accepted: 15/5/2022 Published: 30/1/2023

Abstract

The modern systems that have been based upon the hash function are more suitable compared to the conventional systems; however, the complicated algorithms for the generation of the invertible functions have a high level of time consumption. With the use of the GAs, the key strength is enhanced, which results in ultimately making the entire algorithm sufficient. Initially, the process of the key generation is performed by using the results of n-queen problem that is solved by the genetic algorithm, with the use of a random number generator and through the application of the GA operations. Ultimately, the encryption of the data is performed with the use of the Modified Reverse Encryption Algorithm (MREA). It was noticed that the suggested algorithm provided more sufficient results concerning the key and the strength of security. However, it has lower computational efficiency as compared to the other algorithms.

Keywords Modified Reverse Encryption Algorithm; big data; genetic algorithms; invertible functions; efficient encryption.

تأمين نقل البيانات الضخمة بناءً على التشفير العكسي المعدل والخوارزمية الجينية

ميثاق طالب[1]* ، زيد عثمان[1] ، رشا صبحي[2]
[1]قسم علوم الحاسوب ، كلية العلوم ، الجامعة المستنصرية ، بغداد ، العراق
[2]قسم الهندسة الكهربائية ، كلية الهندسة ، الجامعة العراقية ، بغداد ، العراق

الخلاصة

تعد الأنظمة الحديثة التي تستند إلى وظيفة التجزئة أكثر ملاءمة مقارنة بالأنظمة التقليدية ، ومع ذلك ، فإن الخوارزميات المعقدة لتوليد الوظائف العكسية تتمتع بمستوى عالٍ من استهلاك الوقت. باستخدام الخوارزمية الجينية ، يتم تعزيز القوة الرئيسية ، مما يؤدي في النهاية إلى جعل الخوارزمية بأكملها كافية. في البداية ، تتم عملية إنشاء المفتاح باستخدام نتائج مشكلة n–queen التي تم حلها بواسطة الخوارزمية الجينية ، ويتم إجراؤها باستخدام مولد الأرقام العشوائية ومن خلال تطبيق عمليات الخوارزمية الجينية. في النهاية ، يتم إجراء تشفير البيانات باستخدام خوارزمية التشفير العكسي المعدلة (MREA). لقد لوحظ أن الخوارزمية

*Email: tmethaq@yahoo.com

المقترحة قدمت نتائج أكثر كفاءة فيما يتعلق بالمفتاح وقوة الأمان ، ومع ذلك ، فهي تتمتع بكفاءة حسابية أقل مقارنة بالخوارزميات الأخرى.

1. Introduction

The secure transmission of the data via network became one of the critical and vital issues, because of the increase in the demands for the transmission of the digital media and the unauthorized access of the sensitive data [1]. Cryptography utilizes the mathematical approaches for the authentication. Cryptography has been based upon Encryption/Decryption concepts [2]. In the case where the data has been sent from the sender to the recipient, data is turned into an unreadable form, which has been referred to as the encryption of the data and at the recipient's side data is converted once more into the original form, which is referred to as the data decryption. The encryption as well as the decryption processes requires the key. For protecting the valuable data from the illegal imitations, modifications and eavesdropper's attack, various cryptographic algorithm types have proposed. There are 2 main algorithm types, which are: symmetrical [3] and asymmetrical cryptography [4]. In the former type, 2 different keys have been utilized; one for the encryption, referred to as public key and the other one is for the process of the decryption, referred to as the private key.

In the symmetric models, only one key is utilized for encryption as well as decryption. Applications of both those methods are different as a result of the scheme's efficiency; the symmetric method is mainly utilized to encrypt data as a result of its high efficiency, whereas the asymmetric method is usually utilized for the key distribution and digital signatures. In addition to that, none of the symmetric encryption techniques like the AES, Advanced AES, DES, and IDEA had taken any advantages of the latest advances in the technology of information processing. A variety of today's methods of data encryption [2], [5] can be found in literature. The GA methods [6] are considered a type of those methods.

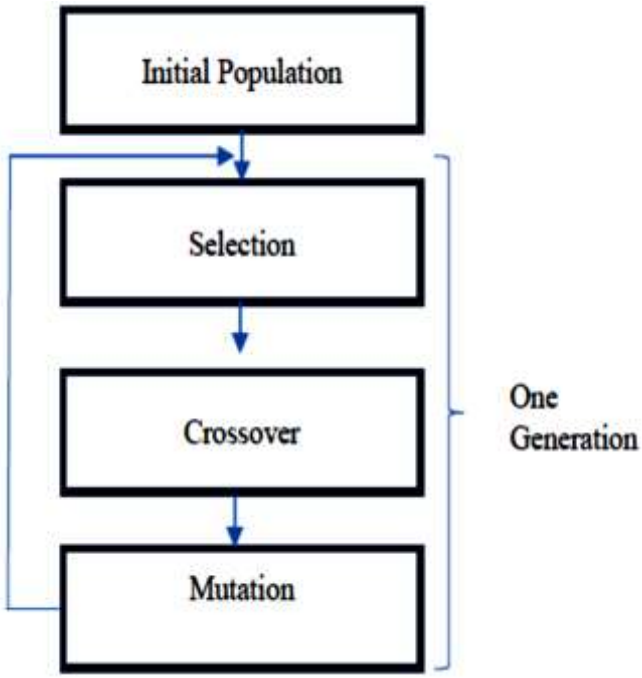

Figure 1: Flow chart of genetic algorithm[7].

There are any methods have been used in the key generation process and one of them depending on the utilizing of Artificial intelligent methods like genetic algorithm, swarm algorithms, ….etc. GAs can be defined as a type of the adaptive search algorithms that take

advantage of the genetics and the natural selection mechanics. GAs have been considered as part of the Evolutionary Algorithms that are utilized for solving the problems of optimization using the biological mechanisms, such as the selection, mutation and crossover [7]. Figure 1 depicts the process of the solution of the problems of optimization with the use of the GAs.

2. Literature Survey

Using the GAs, the majority of researches were carried out by various researchers in the field of key generation and data encryption. Some work has been defined in the following sections.

Turčaník and Javurek [8] , utilized algorithms of data encryption for providing secure communications amongst the users in the modern technology of communications. Hence, in the present work, the potential to use the genetic algorithms for the generation of the cryptographic keys is analyzed. For the mechanism of generating the cryptographic key by utilizing the Tree Parity Machine and GA, which will be the same on the two communication chain sides for the algorithm of encryption, a new approach has been designed for creating an efficiently large population without the use of a high number of synchronizing TPM. Thereby, a wide range of weight values, which may be utilized for the creation of the encryption key, is ensured. Therefore, the encryption key may be quickly changed while encrypting one message, which makes it hard for the attacker to decrypt the encrypted message. The next effort should be aimed towards creating a cryptographic system model, which will utilize the resultant population.

Zahrul Jannat *et al.* [9] performed image encryption with the use of the GA. After that, statistical tests were carried out for visualizing the solution feasibility.
The work that was performed by these researchers had impressive results; however, every one of the research works utilized an existing cryptographic algorithm combined with the operators of the GA. The motivation of the present study is creating an innovative cryptographic algorithm by using GA operations that are easily implemented and secure concerning the attack time and key strength.

Koppu and Viswanatham [10] proposed a chaos-based visual encryption approach that may be applied to the Ultra Sound Medical Images. The adaptive Grey Wolf Optimization (GWO) was utilized for archiving the encryption of the Ultra Sound Medical Images. The robustness of the suggested image encryption was evaluated with a variety of security attacks, including the histogram analysis, key sensitivity, chi-square test, adjacent pixel auto-correlation, and others. In addition, the analytical outcomes were compared to a number of traditional algorithms, such as GWO and GA. The experimental results showed that the suggested approach is faster and less complicated.

Rohini *et al.* [11] presented a new encryption algorithm, which was referred to as the "Reverse Encryption Algorithm (REA)", due to its efficient functioning and simple context. It is more sufficient compared to the other competing algorithms. The REA lowers the added time costs for the decryption and encryption in order to not worsen the efficiency of the data-base system. The REA is a symmetrical stream cipher which may be utilized effectively in data security and encryption.

Pornsing *et al*. [12] examined the need of the dynamic and adaptive cryptographic algorithm for the reduction of the computational costs and improvement of security. They suggested 2 improved AES crypto-systems with the use of the genetic algorithm in the SP

boxes. The AES was modified for accommodating non-linear NN in the SP network. This method ensured improved security and reduction of the computational time and timing attacks.

Tavakoli *et al*. [13] utilized genetic algorithms to encrypt grayscale images. The performance analyses of this method revealed that this algorithm possessed good key sensitivity, statistical results, and the ability for handling plain-text attacks, brute entropy attacks, force attacks, and differential attacks. Venkatesan *et al*. [14] suggested the cryptographic algorithm with the use of the genetic function. In that proposed algorithm, double point cross-over and substitution matrix were utilized for data encryption. This method was carried out in Xilinx13.2 version and verified with the use of the Spartan 3-e kit. Yeun *et al*. [1] were concerned with the security of the electronic data via network. The suggested algorithm integrated genetic algorithms and pseudo-random sequence for data decryption and encryption. The random sequence was obtained with the use of the non-linear shift register. The algorithm's speed and time were estimated in order to observe the results.

Kao *et al*. [15] suggested an innovative algorithm where a pseudo-random number generator was utilized for the key generation. The abovementioned generator uses the computer's current time for the generation of the random numbers. After that, the genetic operations were conducted on the random numbers. Finally, the chosen key was utilized in the AES symmetric algorithm for image encryption. The advantages of the proposed algorithm included reduced computational time, increased efficiency, and key irregularity. An identical key generation approach was followed as well by Kanthavel *et al*. [16]; however, the value of the fitness was estimated through the application of the Gap and Frequency tests in addition to the Hamming distance between 2 binary keys. The algorithm was performed in Java technology, in which 0.50 mutation rate, 100 chromosomes, and 2.50 cross-over rate were applied for this algorithm.

3. N-Queen Problem:

The problem of the 8 queens is the famous NP-complete problem that was initially introduced in 1850 by C. F. Gaus [17], see Figure 2. It was studied by a number of mathematicians in the 19 th century. The principal challenge of this problem lies in the fact that it requires many calculations. The general issue of Queen N was debated by Yaglom and Yaglom in the 1950s [17]. The overall N-Queen problem was characterized by the following stresses in the NxN grid with the following conditions [17]:

1. Only 1 queen can be set in row.
2. Only 1 queen can be set in column.
3. Only 1 queen can be set on diagonal.
4. Just N queens should be set on that grid.

There has been an amount of the methods taken in reviewing that problematic ("like the program development, algorithmic design, AI, and parallel and distributed computing"). Such wide-spread attention in N-Queen problem is partway a result of the features which identifies complex problems, in other words., which contents a group of the universal constraints. In the section lower the proposal of the molecular algorithm will be introduced to solve that problem [6].

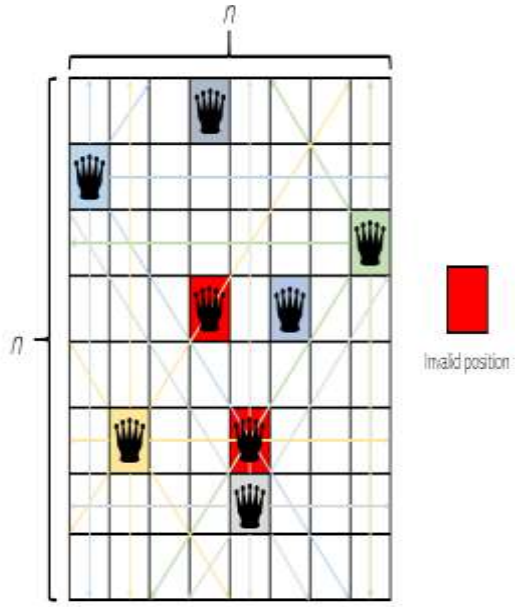

Figure 2: Practically a solution of the 8-queens' problem [18].

4. Genetic Algorithm

The main concept of the GAs is the imitation of the nature's randomness where the process of the natural selection and the natural system's behaviour make a population of the individuals capable of adapting surroundings. It can be said that the individuals' survival and reproduction has been supported through excluding the least fitted individuals. The generation of the population is performed such that an individual with maximum fitness has the highest likelihood of being replicated and the unfitted individual will be discarded according to the threshold that has been set by iteratively applying a group of the stochastic genetic operators [19].

GAs perform the following processes for transformation of population into new population according to the value of the fitness.

A. Cross-over

Which is one of the genetic operators, joining 2 chromosomes for forming a new one. The child chromosome that has been newly generated is made up of the chromosomes from every one of the parents.

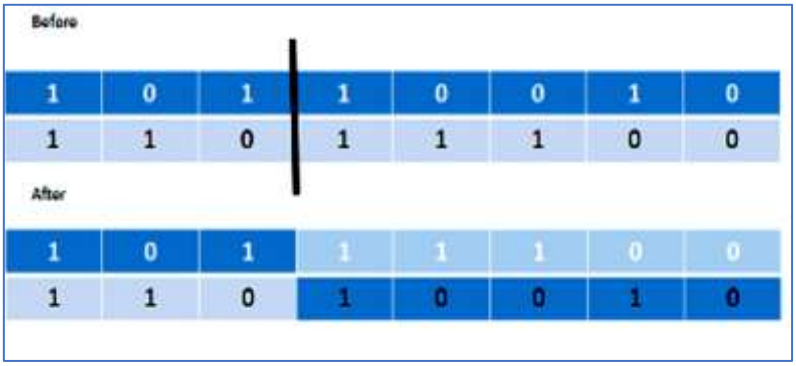

Figure 3: Single point cross-over[10].

Cross-over has been categorized as 1-point, 2-point and uniform cross-over. In the Single Point only a single point of cross-over is chosen for the generation of a new child (Figure 3).

In the 2-Point cross-over, 2 cross-over points are chosen for the generation of the new child (Figure 4). In the Uniform cross-over, the bits are chosen in a uniform way from every parent (Figue 5) [19].

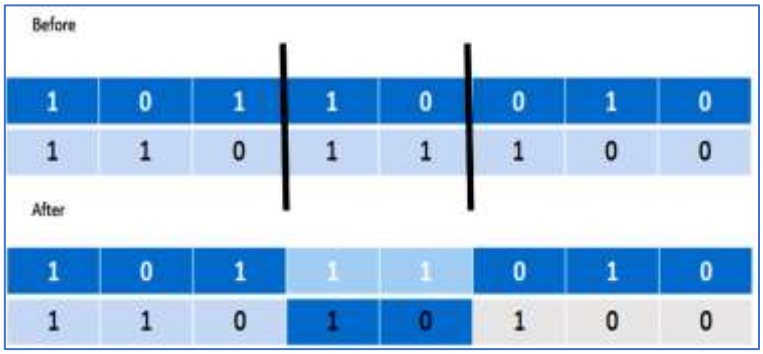

Figure 4: Two point cross-over[10].

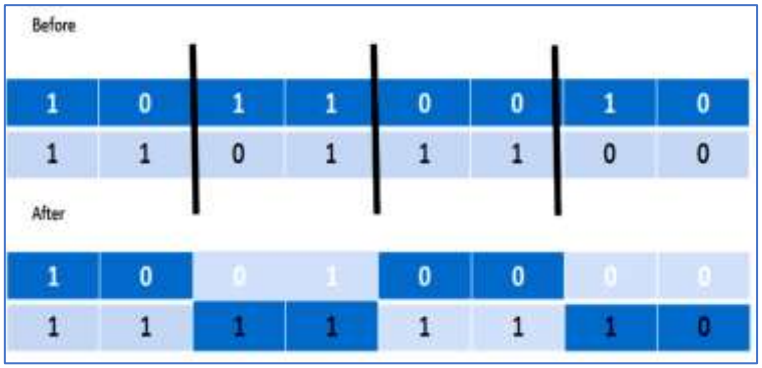

Figure 5: Uniform crossover[10].

B. Mutation

In the mutation following the cross-over, a minimum of 1 bit in very one of the chromosomes is changed (as can be seen from Figure 6) [20]. Which is carried out for reflecting the effects of the surrounding in the natural genetic operation. There are 2 main Mutation types, which are Boundary Mutation and Flipping of Bits. In the latter method, one or several bits are converted from 1 to 0 or from 0 to 1. In the Boundary Mutation, the upper or the lower blocks are randomly swapped in the chromosome [20].

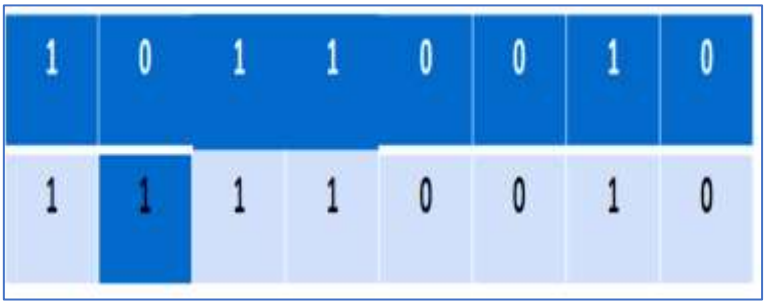

Figure 6: Mutations[11].

C. Selection

In this phase, the chromosomes are selected from population in order to generate the new population. This selection has been based upon the fitness values, the higher the value, the higher are chances of being chosen. The selection has been categorized as Tournament Selection; Roulette-wheel Selection, and Truncation Selection [19].

D. Fitness Function

The fitness function is highly significant for the GAs due to the fact that the good fitness function is beneficial for the efficient exploration of search space and the bad fitness function is confined to the solution of the local optimum. The Fitness Function may be classified as Mutable fitness functions and Constant fitness functions [20].

The Selection of the Key in the cryptography is one of the types of the selection problem and in the case of considering the selection after that; the key that has the maximum level of randomness and fitness is chosen. GA applications are in the search heuristic problems as well, making GAs as reliable algorithms for the encryption of data and key generation.

The opinion that is followed in this paper, is that in the case where quality (i.e. randomness) of pseudo-random numbers that have been produced for the keys is good, then the generated keys will always be non-repeated and entirely randomized and result in ultimately increasing key strength and security.

5. REA encryption algorithm

REA is a new encryption algorithm presented by [11] (Rohini A. Chirde and S. S. Kulkarni) due to its simple context and sufficient working. It has been found more sufficient compared to other competing algorithms. The REA lowers the added encryption and decryption time cost so as not to reduce the data-base system efficiency. The new suggested REA can be defined as a symmetric stream cipher, which may be utilized effectively for data security and encryption. It takes a key with a variable-length, and makes it optimal to secure the data. REA encryption and decryption includes same operations, where only 2 operations differ: a) adding keys to text in encryption and removing keys from text throughout decryption. b) Executing the division operation by 4 on text in encryption and executing several operations on text by 4 in decryption. The operation of the division by 4 is carried out on for the purpose of narrowing the ASCII code table range domain at the conversion of text. It consists of few steps as follow: –

- Add the Key to Plain Text, by just append the Plain to the Key directly
- Convert Combined Text to ASCII Code
- Convert it to Binary Representation with Length of 8 bits for each Segment
- Reverse Binary Bit, which not a real reverse instead it's a NOT Gate
- Convert back to ASCII Code – Divide ASCII Code by 4, Convert the Integer Value to a Char
- Modular ASCII Code by 4
- Add Division Char Result as First Char, and the Modular Result as Second
- Do same for other Digits
- Return So-Called Encrypted Text

6. Proposed Algorithm

The suggested algorithm has been referred to as the Genetic Crypto and has been divided to 3 main steps, which are: Key Generation by solving n-queen problem using genetic algorithm, Data diffusion and Data Encryption (which have been illustrated in Figure 7.

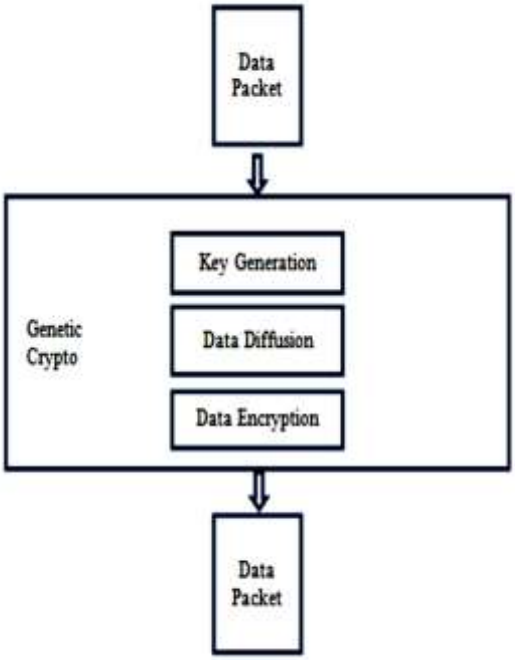

Figure 7: The block diagram of the Genetic crypto.

Genetic operators are utilized in data diffusion as well as key generation. The initial population is produced with the use of the random number generator. For the purpose of the simplicity, 1-point cross-over and bit filliping approaches are utilized for the Cross-over and Mutation respectively. The key fitness value is computed with the use of the Shannon Entropy due to the fact that the entropy is an important randomness property. The proposed algorithm has been carried out using C#.net framework. The interface and the results have been illustrated in Figure 8.

A. Key Generation: the key is 80-128 bits long.

1) 16 characters are randomly produced using a generator of random numbers from A to Z.
2) Every one of the randomly produced characters is converted into binary form (8bits).
3) Result is stored in a 2-D array.
4) Six random prime numbers are produced from 0-100.
5) Every one of the randomly created numbers is converted into the binary form (8bits).
6) Result is stored in a 2-D array.
7) Eight random numbers between 1 and 7 are created for the points of crossover.
8) Those numbers are stored in an array.
9) 1-point cross-over is carried out through taking 1 parent from the random prime number's array and 1 parent from the random characters' array. The point of the cross-over is characterized from the random numbers' array that has been generated in step 8.
10) Repeat Step 9 to the point where there's a parent left for the cross-over.
11) For the Mutation, the bit flipping mutation has been utilized, where the 1st and the last bits of every one of the chromosomes is inverted; which indicates 0 is going to be converted into 1 and the other way around.
12) Repeat Step 11 for all of child chromosomes.
13) Following the Mutation, the Fitness function of every one of the chromosomes is computed with the use of the Shannon's Entropy.
14) The chromosomes with Shannon's (Entropy > 0.95) will be merged and then chosen as the key. If there's none.

15) The chromosome with (entropy > 0.95) then the entire operation will be repeated once more, to the point where there's no best fit key.

B. Original Text Diffusion

1) Data is transformed into the 0,1 form.
2) This binary data is separated to blocks. Every one of the block sizes is 8bits and the number of the blocks (i.e. chromosomes) is the data size /8.
3) Results are stored in a 2-D array.
4) 8 random numbers are generated from 1 to 7 for the cross-over points.
5) Those numbers are stored in an array.
6) 1-point cross-over is conducted between the successive parents in the binary data array. The point of the cross-over is characterized from the random numbers' array, which has been created in step2.5.
7) For the Mutation, the bit flipping mutation has been utilized, where the 1st and the last bits of every one of the chromosomes is inverted.

C. Encryption (Modified REA algorithm has been utilized) which has been included:

1) The Lengths of the key and the data are computed first.
2) The addition of the key and the reverse operation will be carried out.
3) Logical XOR process will be carried out between the key and the results of the step2.
4) The resultant group of the bytes represents the encrypted data

Some work limitations in this study:

a) The randomness is entirely dependent on the generator of the random numbers and it could be pseudorandom number generation. It's only restricted to 16 lettering.
b) The lengths of the key and the data are subjected to the design considerations.

The utilized encryption algorithm much faster than the traditional REA algorithm, it is included direct complement conversion instead of conversion to binary and complemented it.

Algorithm1: REA encryption algorithm
INPUTS: Plain-text (str), Key (key)., f="" // f represents the final encryption vlues//
OUTPUT: Ciphertext.
Begin:
1: str=read all file lines
2: Add the key to plainText (Key + str) let it be k
3: for l=0 to k-1
For i=0 to k(l).length-1 // k(l) represent the current line (record) in the file//
a. cut the elements one by one.
J=k(l).substring(i,1)
b. reverse the previous asci value withot converting it to binary depending on :
a(i)=255-asc(j) // a(i) is atrix include complement values//
c. pplied XOR operation between the a(i) and (kk(i) mod kk.length -1),
i. c= a(i) XOR (key(i) mod key.length -1), and Divide the ascii by 4 let it be T
ii.Convert T to integer let it be d and,
iii.find the remainder of c let it be r(i).
iv. add the result of ii to iii result represented as charter which is f+=chr(d(i) + char r(i)
next
next
6: Return (Encryptedfile).

7. Experimental Result

In this paper, a Modified REA algorithm with GA have been carried out in a large data-base and for algorithm testing, a number of different size files were utilized for the purpose of checking the algorithm's efficiency. Tests have shown that Modified REA has a considerably

higher speed compared to the conventional REA and the AES algorithms as has been listed in Table1. Experimentations have been performed on a mini laptop Intel(R) Core(TM) m7-6Y75 CPU @ 1.20 GHz 1.51 GHz, 8.00GB. The OS that has been utilized is Microsoft Windows 10 professional. The results of the simulation have been carried out according to the data-base. A number of the Big data-base files have been encrypted with the use of original REA method and Modified REA, results of Table2 have shown that Modified REA is considerably faster in encryption compared to the conventional REA.

Table 1: A Comparison for the time of encryption between the original REA and Modified REA, AES in Sec

Database name	Sizein Bytes	Proposed Method time	TraditionalREA time	AES algorithm time
Departm-ent	24000	0.078	0.627	0.2
2014 nation	620000	6.1	48.2	12

The results in Table 1 show that the proposed modified REA algorithm takes less time than the traditional REA and AES algorithm, which is much faster by a proximity 88% and 61% respectively.

Table 2: The Comparison of the Encryption Time Between the Original the Modified REA in Sec

Database name	Size in Bytes	Proposed Method time	Traditional REA time
Department	240000	0.078	0.627
2014 nation	620000	6.1	48.2
Humn drag	3888000	60	476
2011 dept	8956000	210.1	1680.9
Dept state	11792000	193.1	1545

The speed of the algorithm can be characterized by measuring the required encryption and key generation process. The time for the proposed algorithm is shown in Table 2 and Figure 8. The time was measured in (second. millisecond) such as 6.1 means six seconds and 100 ms and the size was measured in bytes.

Function Name	Calls	Total Time	Self Time*
NQueenGA2	1	10.530 s	10.313 s
wrev	49900	0.201 s	0.201 s
uitable	1	0.017 s	0.009 s
uitools\private\uitable_parseold	1	0.007 s	0.002 s
cell.strmatch	5	0.006 s	0.002 s
strmatch	5	0.004 s	0.004 s
uitools\private\usev0dialog	1	0.001 s	0.001 s

Figure 8: Time of key generation process.

Self time can be defined as time which is spent in a function that excludes the time that is spent in the child functions. The self time includes as well the overhead that results from the profiling process.

For the purpose of testing the analysis of the performance for algorithms, statistical properties for the plain as well as the encrypted file have been measured with the use of the 16 statistical tests which are (Frequency Freq., block-frequency BlkFreq., cumulative-sum Cum-Summation, Runs, longest-run LongRun., Rank, Fft, nonperiodic-templates Nonperiodic, Apen, Serial, overlapping-templates overlaping, Universal Univ., lempel-zivLemZiv, linear-Complexity LenComp.), results have been listed in Table 3.

Table 3: The 16 Statistical Test

File Name	Proportion	STATISTICAL TEST
samples size=100 * 500	0.0000	Serial
		LemZiv
	0.9100	LenComp.
	0.9900	Freq.
		Runs
		Fft
	1.0000	Cum-Sum
		LongRun.
		Rank
		BlkFreq
		Nonperiodic
		Overlaping
		Univ.
		Apen
	0.0000	Runs
		Serial
		LemZiv
		Rank
	0.8320	LenComp.
sample size =250 * 500	0.8360	Freq.
		BlkFreq
		Cum-Sum
	0.7560	Fft
	1.0000	LongRun.
		Nonperiodic
		Overlaping
		Univ.
		Apen
sample size=1000 * 200	0.0000	Serial
		LemZiv
		Rank

sample size=500 * 100	0.7570	Runs
	0.8500	Freq.
	0.8720	Cum-Sum
	0.9420	BlkFreq
	0.9990	Fft
	1.0000	LongRun.
		Nonperiodic
		Overlaping
		Univ.
		Apen
		LenComp.
	0.0000	Rank
		LemZiv
	0. 4520	Serial
	0.9960	Runs
	1.0000	Freq.
		BlkFreq
		Cum-Sum
		Fft
		Nonperiodic
	1.0000	Overlaping
		Univ.
		Apen
		LongRun.
		LenComp.

Results of Table3 have shown that the suggested approach method achieved sufficient results; it has passed approximately 11 out of 14 tests, the other 2 tests did not work from the site of the designer.

8. Conclusion

There is much highly important data in a data-base that requires being protected from the attacks. The cryptography is one of the significant mechanisms to secure them. In this paper, a new design for the reinforcement of Modified REA algorithm has been suggested. The Modified REA design differs from original REA in utilization of the key and the reverse operation. A very big benefit from Modified REA, has been found considerably faster compared to original REA and AES algorithms.

Experimental results on benchmark tasks have shown that various starting angles have positive effects on the Sweep clustering and the MCA is more sufficient compared to the other approaches of optimization in solving the CVRP. In the end, the MCA with variant Sweep has been characterized as one of the prominent CVRP solving methods in comparison to the existing related approaches.

9. Acknowledgements

The authors would like to thank the Department of Computer Science, College of Science, Mustansiriyah University for supporting this work.

References

[1] Yeun, L. C., Ismail, W. R., Omar, K. and Zirour, M., "Vehicle Routing Problem: Models and Solutions," *Journal of Quality Measurement and Analysis*, vol. 3, no. 1, pp. 205_218 (2008).

[2] Chen, A., Yang, G. and Wu, Z., "Hybrid Discrete Particle Swarm Optimization Algorithm for Capacitated Vehicle Routing Problem," *Journal of Zhejiang University SCIENCE A*, vol. 7, no. 4, pp. 607_614 (2006). doi: 10.1631/jzus.2006.A0607

[3] Nurcahyo, G.W., Alias, R. A., Shamsuddin, S. M. and Sap, M. N. Md., "Sweep Algorithm in Vehicle Routing Problem for Public Transport," *Journal Antarabangsa* (Teknologi Maklumat), Vol. 2, pp. 51_64 (2002).

[4] Ahmed T., Hasanen S., Zied O., "Meerkat Clan Algorithm: a New Swarm Intelligence Algorithm", *Indonesian Journal of Electrical Engineering and Computer Science* , vol. 10, no. 1, , pp. 354~360, April 2018.

[5] G. W. Nurcahyo, R. A. Alias, S. M. Shamsuddin and M. N. Md. Sap, "Sweep Algorithm in vehicle routing problem for public Transport," *Journal Antarabangsa* (Teknologi Maklumat), vol. 2, pp. 51-64, 2002.

[6] N. Suthikarnnarunai, "A Sweep Algorithm for the Mix Fleet Vehicle Routing Problem," *Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol II, IMECS* 2008, 19-21 March, 2008, Hong Kong.

[7] M. M. A. Aziz, H. A. El-Ghareeb and M. S. M. Ksasy, "Hybrid Heuristic Algorithm for solving Capacitated Vehicle Routing Problem", *International Journal of Computers & Technology*, vol. 12, no.9, pp. 3845-3851, 2014.

[8] Turčaník M., Javurek M. "The Use of Genetic Algorithms for Cryptographic Keys Generation". In: Tagarev T., Atanassov K.T., Kharchenko V., Kacprzyk J. (eds) *Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data*, Vol 84. Springer, Cham., 2021. https://doi.org/10.1007/978-3-030-65722-2_19

[9] Zahrul Jannat, M. Akhand, "Capacitated Vehicle Routing Problem Solving through Adaptive Sweep based Clustering plus Swarm Intelligence based Route Optimization", *Oriental Journal of Computer Science and Technology*, ISSN: 0974-6471, vol. 11, no. 2, 2018.

[10] Srinivas Koppu, Madhu Viswanatham V2, "2D Chaotic Map Based on 2D Adaptive Grey Wolf Algorithm for Ultra Sound Medical Image Security", *International Journal of Intelligent Engineering and Systems*, vol.10, no.1, 2017, DOI: 10.22266/ijies2017.0228.12

[11] Rohini A. Chirde and Prof. S. S. Kulkarni, "Implementing REA Algorithm to Increase Performance of the Encrypted Databases While Query Processing" *International Journal of Computer Science and Information Technologies*, vol. 5, no. 5, pp. 6556-6561, 2014. ISSN: 0975-9646

[12] C. Pornsing, "A Particle Swarm Optimization for the Vehicle Routing Problem," PhD. Thesis, University of Rhode Island, USA, 2014.

[13] M. M. Tavakoli and A. Sami, "Particle Swarm Optimization in Solving Capacitated Vehicle Routing Problem", *Bulletin of Electrical Engineering and Informatics*, vol. 2, no. 4, pp. 252-257, ISSN: 2089-3191, December 2013.

[14] S. R. Venkatesan, D. Logendran, and D. Chandramohan, "Optimization of Capacitated Vehicle Routing Problem using PSO," *International Journal of Engineering Science and Technology* (IJEST), vol. 3, pp. 7469-7477, 2011.

[15] Y. Kao, M. H. Chen and Y. T. Huang, "A Hybrid Algorithm based on ACO and PSO for CVRP", *Research Article,Mathematical Problems in Engineering*, vol. 2012, 2012.

[16] K. Kanthavel and P. Prasad, "Optimization of CVRP by Nested Particle Swarm Optimization" *American Journal of Applied Sciences*, vol. 8, pp. 107-112, 2011.

[17] Sura Mazin Ali, Noor Thamer Mahmood, Samer Amil Yousif; "Meerkat Clan Algorithm for Solving N-Queen Problems"; *Iraqi Journal of Science*, vol. 62, no. 6, pp, 2082-2089, 2021.

[18] Russell S., Norvig P. *Artificial Intelligence: A Modern Approach, chapter 3. Prentice Hall, 2nd edition*, 2003.

[19] H. Nazif and L. S. Lee, "Optimized Crossover GA for Capacitated Vehicle Routing Problem", ELSEVIER, vol. 36, pp. 2110–2117, 2012.

[20] M. Yousefikhoshbakht and E. Khorram, "Solving the vehicle routing problem by a hybrid meta-heuristic algorithm," *Journal of Industrial Engineering International*, vol. 8, no. 11, 2012.