International Journal of Emerging Technology and Innovative Engineering
Volume 5, Issue 1, January 2019 (ISSN: 2394 – 6598)

SURVEY : CRYPTOGRAPHY OPTIMIZATION ALGORITHMS

M. Geetha, K. Akila
PG Students
KRS College of Engineering, Tamilnadu, India.
geethasuresh901@gmail.com

***Abstract*— With the advent of e-commerce, it has become extremely essential to tackle the sensitive issues of affording data security, especially in the ever-blooming open network environment of the modern era. The encrypting technologies of the time-honored cryptography are generally employed to shelter data safety extensively. The term 'cryptography' refers to the process of safeguarding the secret data against access by unscrupulous persons in scenarios where it is humanly impossible to furnish physical protection. It deals with the methods which convert the data between intelligible and unintelligible forms by encryption/decryption functions with the management of key(s). Nowadays cryptographic key management issues that arise due to the distributed nature of IT resources, as well the distributed nature of their control. Recently these issues are solved by optimization algorithms utilized in the cryptographic algorithms. The purpose of this paper is to give a survey of optimal cryptographic keys that can be developed with the help of optimization algorithms, and to address their merits to the real-world scenarios.**

Keywords—Cryptography; Encryption; Decryption; Key Management; Optimization algorithm;

I. INTRODUCTION

Cryptography (also known as cryptology) is an art of achieving security by encoding messages to make them non-readable using different encryption algorithms so that only the intended user can see the original content [19-23].

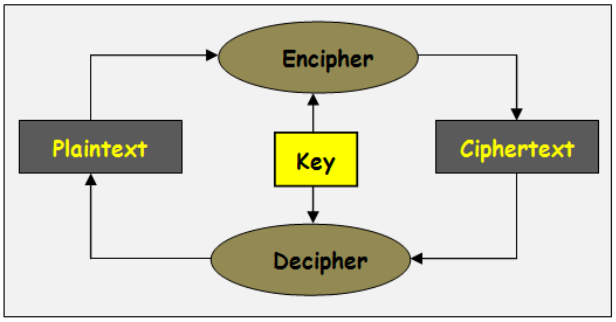


Fig. 1. Architecture of Cryptosystem

The basic block diagram of a cryptosystem is given in figure 1. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense [24-28]. A cryptographic algorithm technically called as cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in association with a key to encrypt the message [1]. A cryptographic algorithm with all possible keys and protocols is known as a cryptosystem. Each security system must supply some security process that guarantees the secrecy of the system [29-32]. Some of the goals that can be achieved by cryptography are as follows: Authentication, Confidentiality, Access Control, Integrity, Non-repudiation, Availability and Accountability. In the cryptographic process encryption and decryption demands a key [33-36]. Some cryptosystems uses the same key together for encryption and decryption called as symmetric key or private key cryptography and asymmetric key or public key cryptography may use different keys together [2]. The mathematical optimization method, which is a best method to choose an element from a group of obtainable alternatives, is used in mathematics, computer science and operation research [37-42]. Simply, an optimization issue contains a set of maximum or minimum real functions from which selecting an input value from an acceptable value and calculating the value of the function [43-46]. Mostly, the optimization theory and methods are used in the field of applied mathematics [47-50]. The optimization method also includes finding the best accessible value of target function from a defined domain or variety of target functions from different type of domain [3]. The main purpose of optimization is to reduce the interval of a point multiplication that depends on the number of required cycles [51-55]. Especially, the replicated arithmetic obstructs are used to improve the parallelism for fundamental process. Most of the execution takes place on algorithm optimization or improved arithmetic architectures finds to be suitable for cryptographic operations [4].

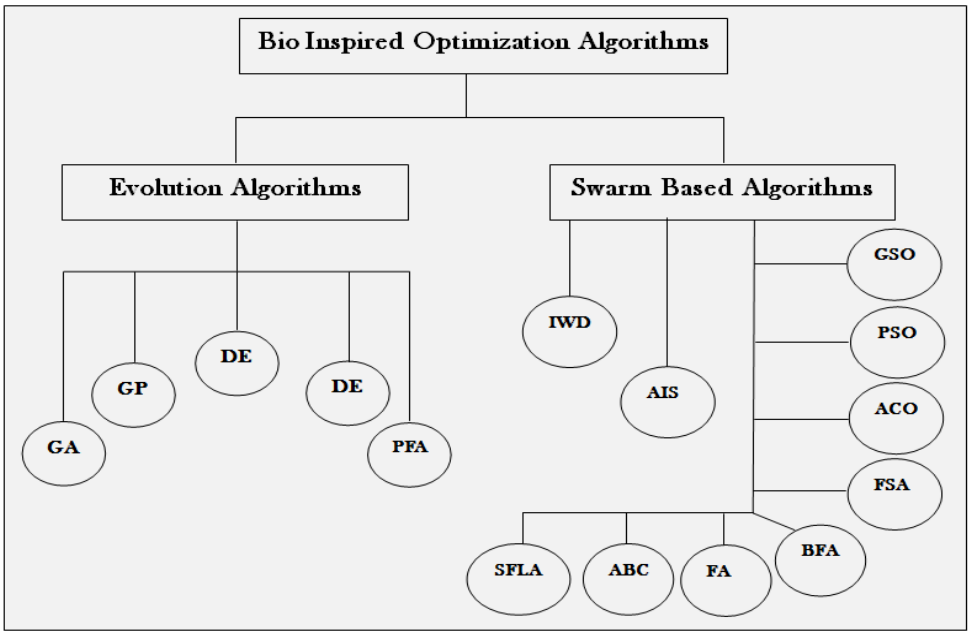
II. SCOPE OF OPTIMIZATION PROBLEMS

In a standard point of view, the process of optimization can be described to find the best solution of the function from the

system within constraints [56]. This process needs the following components such as:

- The result of the function requires a minimized or maximized scalar quantitative process metrics and it is based on systems cost, yield, and profit.
- This converts the optimization issue into a group of equations and inequalities in order of constraints. These constraints are used to comprise a possible area which defines the limitations in process of the system [57].

The predictive model variables must fulfill the constraints. This can be achieved by multiple instances of variable values, guiding to a possible area that is established by a subspace of these variables. These subspaces are classified by a group of decision variables in many engineering issues that can be understood as degree of freedom in the process. Taxonomy of various bio inspired optimization algorithms [16] grouped by the area of inspirations as shown in figure 2.



Evolution		
Evolution Algorithms	GA	Genetic Algorithm
	GP	Genetic Programming
	ES	Evolution Strategy
	DE	Differential Evolution
	PFA	Paddy Field Algorithm
Swarm Based		
Natural River System	IWD	Intelligent Water Drops
Human Immune System	AIS	Artificial Immune System
Convergent Social Phenomenon in Animals	GSO	Group search optimizer
	PSO	Particle Swarm Optimization
	ACO	Ant Colony Optimization
	FSA	Fish Swarm Algorithm
	BFA	Bacterial Foraging Optimization Algorithm
	FA	Firefly Algorithm
	ABC	Artificial Bee Colony
	SFLA	Shuffled Frog Leaping Algorithm

Fig. 2. Taxonomy of various bio inspired optimization algorithms grouped by the area of inspiration

III. OPTIMIZATION ALGORITHMS

Some important traditional and modern optimization algorithms are explained as follows [58-63].

A. Differential Evaluation (DE) Algorithm

DE is mainly used for multi-dimensional real-valued functions, but does not use the gradient of the issue being optimized. This denotes that DE does not possess any optimization issue, but requires classic optimization techniques such as gradient descent and quasi-newton techniques. DE can also be used for optimization issues such as non-continuous, noisy and change over time.

B. Genetic Algorithm (GA)

An algorithm is initiated with a collection of solutions (chromosomes) called population. One population's solution can be used to create a new population. Solutions which are chosen to create new solutions (offspring) are chosen according to their fitness for reproduction and the most suited solution can be selected. In Genetic Algorithm, the fitness operation of the optimization method can be estimated by the chromosome in the hidden layer and neurons. The cross over is created depending on fitness value.

C. Cuckoo Search (CS) Algorithm

The Cuckoo Search algorithm is proposed by entrusting brood parasitism of many cuckoo species i.e., placing their eggs on the nest of host fledglings. The shades can be copied by those female parasitic cuckoos and through the example of host species' eggs. For easiness, it is imagined that there is only one egg at once in a nest. The initial alignment can be interpreted by the accessible egg in the host nest. An egg placed by a cuckoo act as a guide to another alignment created by the strategy.

D. Ant Colony Optimization (ACO) Algorithm

The ACO algorithm is one of the most competent methods that indicate the main aspects of state transition rules and pheromone modernize devices. In each iteration, colonies of ants are sent to a particular place for solution. Each ant works steadily in their state transition rules. Suppose, if an ant completes a work, then the pheromone modernized begins to search another ant with similar strength. But it significantly reduces the opportunities and changes the search methodology [61].

E. Particle Swarm Optimization (PSO) Algorithm

The PSO strategy is engaged to differentiate the perfect solutions from the identified data limits that denote to obtain the perfect equation from the numerical model. The PSO is a population-based search algorithm which is initiated with unique population of randomly-produced solutions which are known as particles. In PSO strategy, the numbers of particles are initially prepared along with initiation of population size after this process updated with new solutions.

IV. CRYPTOGRAPHIC BASED OPTIMIZATION METHODS

In 2012, AartiSoni *et al.* recommended that the cryptography is crucial for ensuring data security with the increased online exchange handling [5]. The research exhibited that the Genetic Algorithm was employed to create a key with the help of a pseudo-irregular number generator. The Random number was created on the premise of current time of the framework. The quality of the way was kept to be great in spite of the entire strategy which is adequate. The authors symmetric key calculation which was utilized for scrambling the image was extremely secure technique for symmetric key encryption. Through the consequences, the effectiveness of strategy was expanded as far as the processing time got obliged and intricacy to assault the message.

K.Shankar *et al.* [6], proposed an efficient method of ECC based image encryption scheme with the aid of optimization technique using the Differential Evolution (DE) algorithm. In this method is used to improve the performance of an image encryption in ECC method, Differential Evaluation (DE) algorithm based optimization process is applied on the private key generation phase. The performance of the image is taken as a fitness value of the optimization process such as PSNR value that shows the efficiency of their method.

N. K. Sreelaja *et al.* proposed the method to encrypt binary image [7] using stream cipher and ant colony optimization technique for key generation. This method reduced the number of keys to be stored and distributed. The character code table is used to encode the keys and characters in the plain text. The result ensures this approach has the capability to encrypt binary images of various sizes.

The authors also proposed swarm intelligence approach [8] or otherwise termed as Ant Colony Optimization key Generation Algorithm (AKGA), for generating keys to encrypt the text message. In this method, stream cipher is used to encode the secret text and AKGA is used for generating keys. Here the keys are reduced and the results of the proposed framework ensure that it has the capability for encrypting original message of varying size.

In another work authors also proposed particle swarm optimization, or otherwise termed as PKGA (Particle swarm optimization Key Generation Algorithm) for generating keys to encrypt original text message [9]. In this method, stream cipher is used to encode the secret text and PKGA is used for generating keys. In this method, keys are reduced to be stored and distributed when compared with vernam cipher. The result of this framework ensures that it has adequate encryption of varying size of original message. When PKGA is compared with AKGA (Ant colony optimization Key Generation Algorithm), the encryption process time is lesser in the former than the latter.

Genetic Algorithm is used by P. Saveetha *et al.* for reducing the computational complexity of the cryptanalysis [10]. Encoding process on the stream cipher using the GA with pseudo random series method consumed lesser memory

and time when compared with the existing Fast Discrete Fourier Spectra approach on stream cipher.

The concept of utilizing Genetic Algorithm and RSA in modified approach is introduced by Abdel-karim S.O. Hassan *et al.* [11]. This method combines both symmetrical (using Genetic optimization) and asymmetrical (using RSA) method to ensure that make the key very complex to reinforce resistance to cryptanalysis. The first operation is symmetrical using GIC to generate the key from plaintext followed by the second operation of the new ciphering technique which is performed by RSA algorithm.

Threshold recovering algorithm for key management was developed by Xuanwu Zhou *et al.* [12]. In this method, encryption was done on private keys which are from KGC and then shared to applier group. The threshold reconstruction of private keys provided protection for the secrecy of private key parameters and also applier identity. In order to make the key management scheme effective, improved authenticated encryption scheme is presented.

K.Shankar *et al.* [13] proposed RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique. In this methods shares of the secret image in visual cryptography process are created by using the multiple shares creation method with ECC. The shares are separately encrypted and decrypted by means of the encryption and decryption technique in line with ECC. In the decryption process we generate the private key by using the cuckoo search optimization technique and for evaluating the performance of the optimization by using the peak signal to noise ratio (PSNR).

V.S.ShankarSriram *et al.* [14] have developed a scheme for scalar multiplication. In this scheme, the Encryption process involves two stages of Modular Multiplication. So, the time required to compute the keys is less and timing-based attacks on the key will be difficult. This scheme can be deployed in Mobile and other wireless devices.

In the method proposed by AartiSoni *et al.*, AES algorithm is used for encrypting and decrypting digital images [15] and GA is used for key generation process. The Key length, for which the test is carried out, is 128 bit long. Longer key sequence will also work but time constraint doesn't permit to check. The time taken to generate key for 300 iteration, with 10 new population each time, 10 crossover and mutation operations each iteration, is75.382 seconds.

In 2014, Sindhuja *et al.* proposed the Genetic Algorithm (GA)-based symmetric key cryptosystem for encryption and decryption [15]. The basic content and the client information (key) were distorted into content matrix and key network separately. Additive matrices were produced by including the content matrix and key network. Linear substitution capacities were connected in the additive matrix to create the transitional figure. At that point, the GA capacities (hybrid and change) were connected to the transitional cipher to deliver the last cipher content. It was accomplished that the symmetric key substitution strategy was utilized to guarantee the secrecy in systems, which was linked and actualized with the assistance of genetic capacities to furnish including security.

J.SaiGeetha *et al.* proposed Artificial Bee Colony Random Number Generator [18], also called as ABCRNG which is fit to all public key cryptosystem to increase the strength of key as well as its security. It is proved through statistical tests that ABC is more efficient than other methods. Randomness of Random numbers is produced in large volumes which are evaluated by run test (Up and Down, above and below mean) method.

V. CONCLUSION

The survey has been investigated over many research papers based on optimization algorithm applied in the cryptographic algorithms. Each authors proposed some of the optimization algorithm is used to optimize the key values in particular cryptographic algorithm. Each method is unique in its own way, which have their own advantages and disadvantages. Based on existing research works the optimization algorithms are used to optimize the key values in complex cryptographic methods like ECC, RSA.etc still remain significantly challenging tasks for the research community.

REFERENCES

[1] Behrouz A. Forouzen, "Cryptography & Network security", McGraw-Hill Companies, pp.1-56, 2007.

[2] Shankar, K., and P. Eswaran. "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm", Artificial Intelligence and Evolutionary Computations in Engineering Systems. Springer India, 2016. 705-714.

[3] https://en.wikipedia.org/wiki/Mathematical_optimization#Computational_optimization_techniques].

[4] A.Durga Bhavani and P.Soundarya Mala, "Optimized Elliptic Curve Cryptography", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 5, pages(s): 412–419, 2012.

[5] Aarti Soni and Suyash Agrawal, "Using genetic algorithm for symmetric key generation in image encryption", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol.1, issue.10, page(s): 137–140, 2012.

[6] K. Shankar, Dr.P.Eswaran: ECC Based Image Encryption Scheme with aid of Optimization Technique using Differential Evolution Algorithm. International Journal of Applied Engineering Research 2015; 10:5:1841-1845.

[7] N.K. Sreelaja and G.A. Vijayalakshmi Pai, "Stream cipher for binary image encryption using Ant Colony Optimization based key generation", Applied Soft Computing, vol. 12, issue.9, age(s): 2879–2895, 2012.

[8] N. K. Sreelaja1 and G. A. Vijayalakshmi Pai, "Swarm intelligence based key generation for stream cipher", Security and Communication Networks, vol. 4, issue.2, page(s): 181–194, 2011.

[9] Sreelaja.N.K and G.A.Vijayalakshmi Pai, "Design of Stream Cipher for Text Encryption using Particle Swarm Optimization based Key Generation", Journal of Information Assurance and Security, vol. 4, page(s): 30–41, 2009.

[10] P. Saveetha, S. Arumugam and K. Kiruthikadevi, "Cryptography and the Optimization Heuristics Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, issue.10, page(s): 408–413, 2014.

[11] Abdel-karim S.O. Hassan, Ahmed F, Shalash and Naglaa F. Saudy, "Modifications on RSA Cryptosystem Using Genetic Optimization", International Journal of Research and Reviews in Applied Sciences, vol.19, issue.2, page(s): 150, 2014.

[12] Xuanwu Zhou, "Scheme Optimization in Key Management with Cryptograph Methods", Applied Mechanics and Materials, vol. 20, page(s): 539–545, 201.

[13] Shankar, K., and P. Eswaran. "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique", Journal of Circuits, Systems and Computers 25.11 (2016): 1650138.

[14] V.S.Shankar Sriram, S.Dinesh and G.Sahoo, "Multiplication Based Elliptic Curve Encryption Scheme with Optimized Scalar Multiplication (MECES)", International Journal of Computer Applications, vol.1, no. 11, page(s): 65–70, 2010.

[15] Aarti Soni and Suyash Agrawal, "Key Generation Using Genetic Algorithm for Image Encryption", International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 2, issue. 6, page(s):376–383, 2013.

[16] Binitha S, S Siva Sathya, "A Survey of Bio inspired Optimization Algorithms ", International Journal of Soft Computing and Engineering, Volume.2, Issue.2, page(s):137-151, May 2012.

[17] Sindhuja K and Pramela Devi S, "A symmetric key encryption technique using genetic algorithm", International Journal of Computer Science and Information Technologies, vol. 5, issue.1, page(s): 414–416, 2014.

[18] J.Sai Geetha and D.I.George Amalarethinam, "ABCRNG-Swarm Intelligence in Public key Cryptography for Random Number Generation", International Journal of Fuzzy Mathematical Archive, vol. 6, issue.2, page(s): 177–186, 2015

[19] Jansirani, A., Rajesh, R., Balasubramanian, R., & Eswaran, P. (2011). Hi-tech authentication for pslette images using digital signature and data hiding. Int. Arab J. Inf. Technol., 8(2), 117-123.

[20] Shankar, K., Lakshmanaprabu, S. K., Gupta, D., Khanna, A., & de Albuquerque, V. H. C. Adaptive optimal multi key based encryption for digital image security. Concurrency and Computation: Practice and Experience, e5122.

[21] Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications, 1-15.

[22] K. Shankar, Lakshmanaprabu S. K, "Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm", International Journal of Engineering & Technology, Volume. 7, Issue. 9, page(s): 22-27, 2018.

[23] Gupta, D., Khanna, A., Shankar, K., Furtado, V., & Rodrigues, J. J. Efficient artificial fish swarm based clustering approach on mobility aware energy efficient for MANET. Transactions on Emerging Telecommunications Technologies, e3524.

[24] Uthayakumar, J., Metawa, N., Shankar, K., & Lakshmanaprabu, S. K. (2018). Financial crisis prediction model using ant colony optimization. International Journal of Information Management.

[25] Uthayakumar, J., Metawa, N., Shankar, K., & Lakshmanaprabu, S. K. (2018). Intelligent hybrid model for financial crisis prediction using machine learning techniques. Information Systems and e-Business Management, 1-29.

[26] Shankar, K., Elhoseny, M., Kumar, R. S., Lakshmanaprabu, S. K., & Yuan, X. (2018). Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. Journal of Ambient Intelligence and Humanized Computing, 1-13.

[27] Lakshmanaprabu, S. K., Mohanty, S. N., Shankar, K., Arunkumar, N., & Ramirez, G. (2019). Optimal deep learning model for classification of lung cancer on CT images. Future Generation Computer Systems, 92, 374-382.

[28] Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications, 1-15.

[29] Avudaiappan, T., Balasubramanian, R., Pandiyan, S. S., Saravanan, M., Lakshmanaprabu, S. K., & Shankar, K. (2018). Medical image security using dual encryption with oppositional based optimization algorithm. Journal of medical systems, 42(11), 208.

[30] Lakshmanaprabu, S. K., Shankar, K., Gupta, D., Khanna, A., Rodrigues, J. J., Pinheiro, P. R., & de Albuquerque, V. H. C. (2018). Ranking analysis for online customer reviews of products using opinion mining with clustering. Complexity, 2018.

[31] Karthikeyan, K., Sunder, R., Shankar, K., Lakshmanaprabu, S. K., Vijayakumar, V., Elhoseny, M., & Manogaran, G. (2018). Energy consumption analysis of Virtual Machine migration in cloud using hybrid swarm optimization (ABC–BA). The Journal of Supercomputing, 1-17.

[32] Shankar K, Mohamed Elhoseny, Lakshmanaprabu S K, Ilayaraja M, Vidhyavathi RM, Mohamed A. Elsoud, Majid Alkhambashi. Optimal feature level fusion based ANFIS classifier for brain MRI image classification. Concurrency Computat Pract Exper. 2018;e4887.https://doi.org/10.1002/cpe.4887

[33] Lydia, E. L., Kumar, P. K., Shankar, K., Lakshmanaprabu, S. K., Vidhyavathi, R. M., & Maseleno, A. (2018). Charismatic Document Clustering Through Novel K-Means Non-negative Matrix Factorization (KNMF) Algorithm Using Key Phrase Extraction. International Journal of Parallel Programming, 1-19.

[34] Lakshmanaprabu SK, K. Shankar, Ashish Khanna, Deepak Gupta, Joel J. P. C. Rodrigues, Plácido R. Pinheiro, Victor Hugo C. de Albuquerque, "Effective Features to Classify Big Data using Social Internet of Things", IEEE Access, Volume.6, page(s):24196-24204, April 2018.

[35] Nur Aminudin, Andino Maseleno, K. Shankar, S. Hemalatha, K. Sathesh kumar, Fauzi, Rita Irviani, Muhamad Muslihudin, "Nur Algorithm on Data Encryption and Decryption", International Journal of Engineering & Technology, Volume. 7, Issue-2.26, page(s): 109- 118, June 2018.

[36] Pandi Selvam Raman, K. Shankar, Ilayaraja M, "Securing cluster based routing against cooperative black hole attack in mobile ad hoc network", International Journal of Engineering & Technology, Volume. 7, Issue. 9, page(s): 6-9, 2018.

[37] K. Sathesh Kumar, K. Shankar, M. Ilayaraja, M. Rajesh, "Sensitive Data Security in Cloud Computing Aid of Different Encryption Techniques", Journal of Advanced Research in Dynamical and Control Systems, Volume. 9, Issue. 18, page(s): 2888-2899, December 2017.

[38] I. Ramya Princess Mary, P. Eswaran, K. Shankar, "Multi Secret Image Sharing Scheme based on DNA Cryptography with XOR", International Journal of Pure and Applied Mathematics, Volume 118, No. 7, page(s) 393-398, February 2018.

[39] K. Shankar, Mohamed Elhoseny, E. Dhiravida chelvi, SK. Lakshmanaprabu, Wanqing Wu, , IEEE Access, Vol.6, Issue.1, page(s): 77145-77154, December 2018. https://doi.org/10.1109/ACCESS.2018.2874026

[40] E. Laxmi Lydia, K. Shankar, J. Pamina, J. Beschi Raja, "Correlating NoSQL Databases With a Relational Database: Performance and Space", International Journal of Pure and Applied Mathematics, Volume 118, No. 7, page(s) 235-244, February 2018.

[41] K. Shankar, G. Devika and M. Ilayaraja, "Secure and Efficient Multi-Secret Image Sharing Scheme based on Boolean Operations and Elliptic Curve Cryptography", International Journal of Pure and Applied Mathematics, Volume 116, Issue. 10, page(s): 293-300, October 2017.

[42] M. Ilayaraja, K. Shankar and G. Devika, "A Modified Symmetric Key Cryptography Method for Secure Data Transmission", International Journal of Pure and Applied Mathematics, Volume 116, Issue. 10, page(s): 301-308, October 2017.

[43] G. Devika, M. Ilayaraja and K. Shankar, "Optimal Radial Basis Neural Network (ORB-NN) For Effective Classification of Clouds in Satellite Images with Features", International Journal of Pure and Applied Mathematics, Volume 116, Issue. 10, page(s): 309-329, October 2017.

[44] K. Shankar. "An Optimal RSA Encryption Algorithm for Secret Images", International Journal of Pure and Applied Mathematics, Volume 118, No. 20 page(s): 2491-2500, 2018.

[45] M Elhoseny, X Yuan, Z Yu, C Mao, H El-Minir, and A Riad,. Balancing Energy Consumption in Heterogeneous Wireless Sensor Networks using Genetic Algorithm", IEEE Communications Letters, IEEE, (2015), 19(12), pp, 2194 -2197.

[46] Mohamed Elhoseny, Khaled Elleithy, Hamdi Elminir, Xiaohui Yuan, and Alaa Riad. Dynamic Clustering of Heterogeneous Wireless Sensor Networks using a Genetic Algorithm, Towards Balancing Energy Exhaustion. International Journal of Scientific & Engineering Research, (2015), 6(8), pp, 1243-1252.

[47] Mohamed Elhoseny, Xiaohui Yuan, Hamdy K El-Minir, and AM Riad, " Extending self-organizing network availability using genetic algorithm", In 2014 International Conference on Computing, Communication and Networking Technologies (ICCCNT), (2014),pp, 11-13.

[48] K. Shankar and P.Eswaran. "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm", Advances in Intelligent Systems and Computing, Springer, Volume: 394, Page(s): 705-714, 2016.

[49] Noura Metawaa, M. Kabir Hassana, and Mohamed Elhoseny. Genetic algorithm based model for optimizing bank lending decisions. Expert Systems with Applications, 2017, 80, pp, 75–82.

[50] Xiaohui Yuan, Daniel Li, Deepankar Mohapatra, Mohamed Elhoseny. Automatic removal of complex shadows from indoor videos using transfer learning and dynamic thresholding. Computers and Electrical Engineering, 2017, 70, pp, 813-825.

[51] Hamid Reza Boveiri, Raouf Khayami, Mohamed Elhoseny, M. Gunasekaran. An efficient Swarm-Intelligence approach for task scheduling in cloud-based internet of things applications, Journal of Ambient Intelligence and Humanized Computing, 2018. https://doi.org/10.1007/s12652-018-1071-1

[52] K. Shankar and P.Eswaran. "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography", Procedia Computer Science, Elsevier, Volume: 70, Page(s): 462-468, 2015.

[53] Farahat I.S., Tolba A.S., Elhoseny M., Eladrosy W. Data Security and Challenges in Smart Cities. In: Hassanien A., Elhoseny M., Ahmed S., Singh A. (eds) Security in Smart Cities: Models, Applications, and Challenges. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham, 2019. https://doi.org/10.1007/978-3-030-01560-2_6

[54] Elhoseny M., Hassanien A.E. Expand Mobile WSN Coverage in Harsh Environments. In: Dynamic Wireless Sensor Networks. Studies in Systems, Decision and Control, Springer, Cham, 2019, 165,pp, 29-52. https://doi.org/10.1007/978-3-319-92807-4_2

[55] Mohamed Elhoseny, Xiaohui Yuan, Hamdy K. El-Minir, Alaa Mohamed Riad. An energy efficient encryption method for secure dynamic WSN. Security and Communication Networks, 2016, 9(13), pp, 2024-2031.

[56] K. Shankar and P.Eswaran, "A New k out of n Secret Image Sharing Scheme in Visual Cryptography", 2016 10th International Conference on Intelligent Systems and Control (ISCO), IEEE, page(s): 369–374, 2016.

[57] Mohamed Elhoseny, Hamdy Elminir, Alaa Riad, XiaohuiYuana. A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption. Journal of King Saud University - Computer and Information Sciences, 2016, 28(3), pp, 262-275.

[58] Sriti Thakur, Amit Kumar Singh, Satya Prakash Ghrera, Mohamed Elhoseny. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications, Multimedia Tools and Applications, 2018. https://doi.org/10.1007/s11042-018-6263-3

[59] Elhoseny M., Hassanien A.E. Hierarchical and Clustering WSN Models: Their Requirements for Complex Applications. In: Dynamic Wireless Sensor Networks. Studies in Systems, Decision and Control, Springer, Cham, 2019, 165, pp, 53-71. https://doi.org/10.1007/978-3-319-92807-4_3

[60] K. Shankar and P.Eswaran. "A Secure Visual Secret Share (VSS) Creation Scheme in Visual Cryptography using Elliptic Curve Cryptography with Optimization Technique". Australian Journal of Basic and Applied Sciences. Volume: 9, Issue.36, Page(s): 150-163, 2015.

[61] Mohamed Elhoseny, Noura Metawa and Aboul Ella Hassanien, An automated information system to ensure quality in higher education institutions, Proceedings of 12th International Computer Engineering Conference (ICENCO), IEEE, 2016, pp, 196 - 201, https://doi.org/10.1109/ICENCO.2016.7856468

[62] AM Riad, Hamdy K El-Minir, Mohamed Elhoseny, "Secure Routing in Wireless Sensor Networks: A State of the Art", International Journal of Computer Applications, 67(7), 2013

[63] Mohamed Elhoseny, HAMDY K Elminir, AM Riad, and Xiaohui Yuan, "Recent advances of secure clustering protocols in wireless sensor networks", International Journal of Computer Networks and Communications Security, 2(11): 400-413, 2014.

[64] Raja, J. Beschi, S. Chenthur Pandian, and J. Pamina. "Certificate revocation mechanism in mobile ADHOC grid architecture." *Int. J. Comput. Sci. Trends Technol* 5 (2017): 125-130.

[65] Raja, J. Beschi, and K. Vivek Rabinson. "Iaas for Private and Public Cloud using Openstack." *International Journal of Engineering* 5.04 (2016).

[66] Raja, J. Beschi, and V. Vetriselvi. "Mobile Ad Hoc Grid Architecture Based On Mobility of Nodes." *International Journal of Innovative Research in Computer and Communication Engineering* 2 (2014): 49-55.