

Medical Imaging Data Security using Modified Honey Encryption Algorithm with Ant-Lion Optimization Technique

¹G. Jayahari Prabhu , ²B.Perumal

Abstract--- Security is the one of the significant thing for transmitting the restorative information. Since it contains some extra data of patients. Medical Imaging Data Security is a Necessary system for secure or safeguards the sensitive information and their related patient data and the information are put away and transmitted over the open system. Numerous cryptographic calculations are accessible, and they fall under symmetric, asymmetric and other procedures. To choose an algorithm for secure information correspondence, the algorithm should to give higher Privacy, security and better effectiveness. Here in medical imaging data, modified honey encryption uses DTE (Distribution Transforming Encoder). DTE encodes or decodes the message space using the Specified function and is used to scramble the restorative medical data. After that the Ant-Lion optimization is used to overhaul the keys. The presentation of the proposed methodology is assessed utilizing different parameters such as Entropy, Peak Signal to Noise ratio (PSNR), Correlation Coefficient (CC) and Mean Square error (MSE)

Keywords--- Medical Imaging data, Modified Honey Encryption Algorithm, Ant-Lion Optimization

I. INTRODUCTION

With the innovation in the field of medical imaging data transmission, the requirement for sharing the medical imaging data information has expanded altogether with many standard algorithms. Security is the main issue while exchanging the restorative medical data progressively in the medical applications. With the extensive enhancements of communication and technologies, medical imaging and digital image application can trade over the internet. Cryptographic design and other calculation approaches are in this basic manner for constant security. And the medical image transmission will store in the open systems. Like other sensitive information restorative medical image expect security to transmit the required through public networks. Through the need of fast and safe determination is much significant in the medicinal field [1]. These days, the transmission of medical image is a normal procedure and it is critical to find a helpful strategy to transmit over the system [2]. In the protected communication of medical images, there are about current security calculations that might to be used [3]. The information can be utilized to give different security such as secrecy, information, uprightness, authentication, authorization and non-repudiation [4]. Because of different issues with correspondence security

¹ Research Scholar of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India, jayahariprabhu@gmail.com

²Associate Professor of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India, palanimet@gmail.com

[5]. Most basic encryption calculations will use as content information or matched information. The primary ciphers are not appropriate figures to be utilized. Also, these primary figures require much computing time and high system power. The significance of encryption for the medical information must be secured [6]. Medical images will be performed with the compelling of Modified honey encryption the cryptographic task can help in giving the necessary security data by figuring restorative picture to some unintelligible configuration utilizing symmetric and asymmetric key encryption scheme. Both single and multi-objective technique will laid with encryption technique [7]. optimization problems with multiple objectives; here proposed ant-lion optimization technique, although the existing algorithms can take care of an assortment of problems, as per the NFL theorem, they are not ready to take care of all optimization problems. This work proposes the multi-objective with the would like to more readily take care of some security issues. Here the optimization algorithm is used to decrypt the input images [8]. The data will be securely transmitting it between the sender and receiver [9]. simulation results gives the better execution of the encryption model.

II. LITERATURE REVIEW

In this work the data have been transferred secretly into the multimedia like audio, video and image To hide a quantum secret image into a quantum cover image, a major steganography is approached [10]. To increase the security level inspired with the algorithm. In this study, for selecting an image security the Homomorphic Technique with optimal key is utilized [11]. For better security approach, chaotic encryption on watermarked medical image is encrypted. By applying NSCT, the cover image is divided and also having maximum entropy [12]. In this proposed work, Genetic Algorithm-based FCM-S1 is used which takes into consideration the effect of the neighborhood pixels around a central pixel and exploits this property for noise reduction. [13]. This paper affords an reply for coinciding medical image coding and compression. The coding overall performance originates from every techniques, whereas the compression end result is accomplished with the aid of cesium. And its leads to Three-dimensional (3-D) cat map is used for key move key generation [14]. The rule utilizes substitution-based cryptography and transposition-based cryptography to attain high degree of entropy within the encrypted watermarked pictures. The operation of the rule is predicated on dividing the initial medical image every which way into 2 halves, every of that is allotted a distinct watermark. One among the watermarks is embedded before cryptography and also the other watermark is embedded when cryptography [15]. Applying security to the transmitted clinical image is vital to safeguard the privateness of patients. Throughout transmission it needs cryptography, and watermarking to achieve secrecy, and integrity. Enhancing cryptography want to use a coding set of rules that symbolize an extended time towards varied attacks. The projected approach relies on remainder theorem as a backbone for this methodology. This methodology achieves high level of protection and stands towards individual attacks for an extended time [16]. Ant Lion improvement (ALO) could be a novel meta-heuristic impelled by searching mechanism of Emmet lions in nature. Numerous emission gases thought-about for the case studies are SO_x, Roman deity and CO_x. The planned technique is applied on totally different take a look at systems for determination the

MOGS.Comparison of the obtained results is distributed with alternative techniques explicit in literature that shows that ALO is effective to solve MOGS. [17].The proposed algorithm well explains and combines the need of flower pollination algorithm and the ability of the original flower pollination algorithm and Nelder–Mead simplex method together by integrating these two methods in a very simple way. [18].

III. METHODOLOGY

Medical information, random number accepts as a best part of the nature of assumption and it is signified by encryption key [19].Some of security issues identified with Medical imaging and by transmitting, to keep the information in safe and secure manner. Mainly the confirming of medical images will guarantee protection, protection of medical data and information put away in a sequence framework, for this exceeding requirements.Modified Honey Encryption for medical imaging security is shown in Fig1.Consider Modified Honey encryption and additionally Ant-lion for the proposed work. This ALO is raised to develop both the key, after the decryption process, the yield image will be the first image by utilizing the PSNR and the other measures [20].

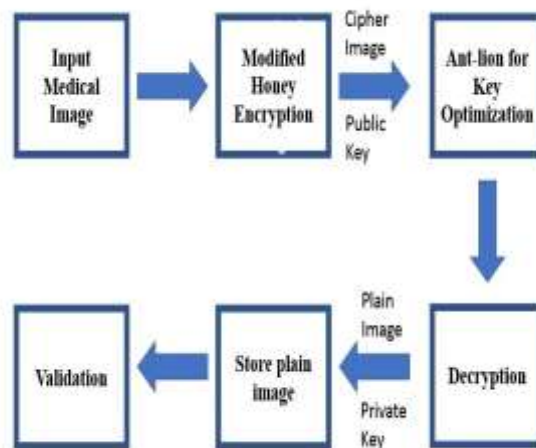


Figure 1: Block Diagram for Proposed Work

A. Modified Honey encryption initial process

To get better Peak signal to Noise Ratio with encrypted images.Modified honey algorithm is more protected than the other algorithms. The Encryption technique is carrying out with the brute force attack. Brute force attack is trial or error method to obtain info such as user password or pattern. Honey encryption uses DTE (Distribution Transforming Encoder). DTE encodes or decodes the message space using the Specified function.DTE is applied to message to obtain the seed. The obtained seed is encrypted using Cipher key that will give HE-Cipher text.

B. Encryption process

Let us consider A and B, where A is supposed to send medical information to next end. During encryption process, the user will get the significant message (M) and will be mapped to the hash estimation(S) created utilizing SHA256 validation. Some valid strings are mapped and the random valid strings (M, M1, M2,) mapped with seed esteem (S, S1, S2,).

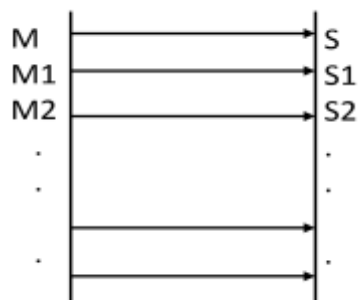


Figure 2 : Mapping between string and Seed values

The SHA256 is hashed with another esteem will generate randomly. This seed value will be received by public key of receiver B and then it is encrypted with the receiver B. Then it is connected with xor value of mapped function.

Keys raised with other value R i.e.

$$C = H(K, R) \oplus S \parallel \text{RSA}(\text{Pub}, R) \quad (1)$$

Where H is the hash Function; K denotes the Key and S is the string .The Receiver will get the resultant cipher text [19].The Hash value of Key K with other value R, S and hash value of key is raised with the seed values S1, S2, S3 and hash value of key K1, k2, k3 ...with salt R and the bogus key value will be K1, K2, K3.. i.e.

$$S_i = H(K, R) \oplus S \oplus H(K_i, R) \quad (2)$$

C. Decryption process

It will generate their initial bits which contains some Xor mapped with the Hash value of key.RSA encrypted random string will be added to it. Initially to get the random string, the cipher text with his public at the receiving aspect it will decrypt with some of the RSA part.



Figure 3: Decrypting RSA

By using the K the random string R will be decrypted. it will receive and generate the hash value. 256 bit of cipher text will be the resultant value .while reverse mapping is done to generate the value and therefore

$$H(K,R) \oplus S \oplus H(K, RSA(PRb, RSA(Pub, R))) = S \quad (3)$$

The value of attacker both the Cryptographic key and

decrypted random string R knows the level [20].If the attacker tries to decrypt the information using the key k1, k2, k3, then the result is value is

$$H(K,R) \oplus S \oplus H(K1, RSA(PRb, RSA(Pub, R))) = S1 \quad (4)$$

Bogus message will be S1 maps to M1 .

D.Key generation stage

The Key generation which contains by selecting some parameters and also creating both public and private key. high reliability and low cost Ant Lion optimization is identified here in the key generaion [20].

For encrypting the Medical information,In the public key cryptosystem the extra operation is done with the homomorphic encryption [21]. additionally, Key generation to decryption are the four functions used here. By decrypting the Medical information or data of honey; honey provides the same outcome on the first one.

E. KeyUtilization

To choose the extra parameters with the selection here it will register both the public and private key will use the Generation algorithm continues [20].

$$(G \text{ pk and } G \text{ sk}) \quad (5)$$

Here Key K uses the generation algorithm and therefore

$$K = cd \text{ and } w = \text{lcm}(r - 1, s - 1) \quad (6)$$

Random keys for encryption and decryption will be used for Antlions.Here it uses open walk around pros, building traps, Ant in a catch,latching prey and remaking traps.this fundamentals are used for the key generation.

1. Keys for Crptographic process

In the Key generation it will pass through the space and make use of the characteristic chance, the traps of the antlions will control the Random walks .and the corresponding to their fitness Ant-lions can assemble openings as

$$\text{Key}(K) = \{\alpha k1, \alpha k2, \alpha k3 \dots \dots \alpha kn\} \quad (7)$$

Every ant can be got with every iteration with the fittest antlion. To reproduce down ants towards antlions the scope of the fittest antlion subjective walk is diminished partially.

2.Robustness

Entropy is a sensible proportion of components that will be used in the Medical Image.Medical Image having most critical entropy and least CC is choosen as a best secret message and subsequently, this Medical image will be sent to the objective and it will raised with the others [20].

$$\text{Fitness} = \text{MAX}(\text{Entropy}) \quad (8)$$

Here N is the Number of gray level identicated and Pi is the Probability of i th gray level medical representation.

3 .Key updation for ALO

To replicate more connections, ants are necessary to move above the certain place. and antlions are acceptable and follow them and bend up audibly. In the view of the underside condition Random walks of antlions were introduced [20]

$$\text{Opt_key}=\{0,\text{cs}(2r(t11)),\text{cs}(2r(t21))\dots\text{cs}(2r(t1)} \quad (9)$$

$$\text{ar}(t)=\begin{cases} 1 & \text{if } \text{frand} > 0.5 \\ 0 & \text{if } \text{frand} \leq 0.5 \end{cases} \quad (10)$$

Here Total Cumulative(cs) and n is the Number of Iteration r(t) Iterative function

During the updation the position of ants directly utilized.The above condition can't be for the direct updation.Min-Max Normalization process can be done with a particular ultimate objective to keep the process around the interest space, they are standartized using will be

4. Building traps by Antlion

For greater fitness the highest possibility of catching ants will be represented using the other. here, the casual walk of ant is leaded by the Ant lion and therefore, the rearrangement of a specified ant lion will be appeared[21].

$$K,n(I)=Rk(1)+RE(1) /2 \quad (11)$$

5. Catching and transformation

The Ant fitness assessment of the key is maximum than the fitness of antlion, At the point when the antlion gets the maximum fitness

$$k(t) \text{ if } k1(t) < f(k2(t)) \quad (12)$$

The smallest to largest fitness value is obtained by concentrating all fitness value .The fitness value is sorted from smallest to largest fitness. The expanding number of ants in the middle of the iteration will be influenced. Ideal keys which are concerning point of antlions that is to be concentated. For security analysis Medical images were collected from hospital and some security measures are examined here.

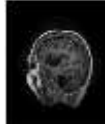

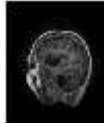
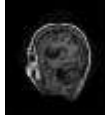

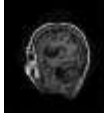
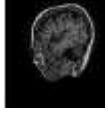



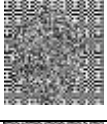




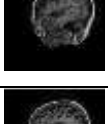
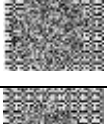
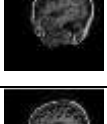
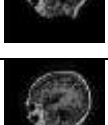

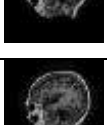












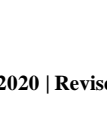

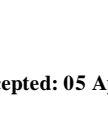
$$\text{PSNR}=10\log(255^2 |MSE) \quad (13)$$

$$\text{MSE}=\sum\left(\frac{1}{\text{Dim}} (\sigma_{i-D_i})^2\right) \quad (14)$$

$$\text{CC}=\frac{\sum_{i=1}^N (I_i-d(I))-(m_i-d(m))}{\sqrt{\sum_{i=1}^N (I_i-d(I))^2-m_i-d(m))^2}} \quad (15)$$

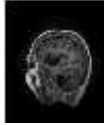

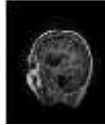
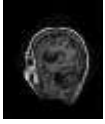
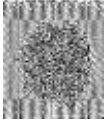

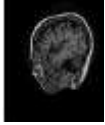











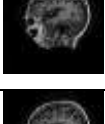

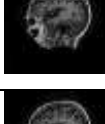
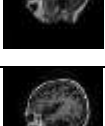


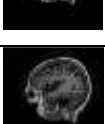

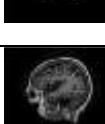



$$\text{Entr}=\sum_{i=0}^{2^N-1} P_i \log\left(\frac{1}{p_i}\right) \quad (16)$$



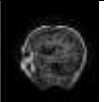
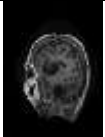


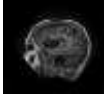


TABLE 1: Performance Measures of blowfish with Ant lion optimization algorithm

<i>Input</i>	<i>Encrypted Images</i>	<i>Decrypted Images</i>	<i>PSNR</i>	<i>MSE</i>	<i>CE</i>	<i>Entropy</i>
			59.61	0.019	1	7.80
			58.90	0.013	0.99	8.02
			56.22	0.02	0.97	7.91
			57.86	0.031	0.96	7.85
			57.78	0.06	1	8.02
			59.31	0.05	0.97	7.51
			57.32	0.08	0.96	7.85
			58.32	0.02	0.94	8.02
			58.90	0.11	1	7.94
			57.83	0.02	0.97	8.02
			59.62	0.05	0.97	7.85
			57.79	0.08	1	7.98

			58.90	0.02	0.94	7.85
---	---	---	-------	------	------	------

TABLE 2: Performance Measures of Modified honey algorithm with Ant lion optimization algorithm

<i>Input</i>	<i>Encrypted Images</i>	<i>Decrypted Images</i>	<i>PSNR</i>	<i>MSE</i>	<i>CE</i>	<i>Entropy</i>
			59.69	0.011	1	7.80
			59.93	0.011	0.99	8.02
			57.21	0.02	0.97	7.91
			58.89	0.019	0.98	7.85
			58.79	0.04	1	8.02
			59.91	0.02	0.99	7.51
			58.31	0.02	0.97	7.85
			58.39	0.02	0.98	8.02
			58.94	0.11	1	7.94
			58.81	0.02	1	8.02

			59.69	0.04	0.97	7.85
			59.79	0.04	1	7.98
			59.90	0.02	0.98	7.85

IV. RESULTS

In the existing system the Medical image is encoded with the dual encryption with Opposition based flower pollination (OFP). The dual Encryption algorithms which transmit the medical image protected with some attacks. Here in the Modified Honey encryption this transmits the medical images in safe and secure way. Towards the end decoding is done so far with high transmission

TABLE 1. Comparative analysis results

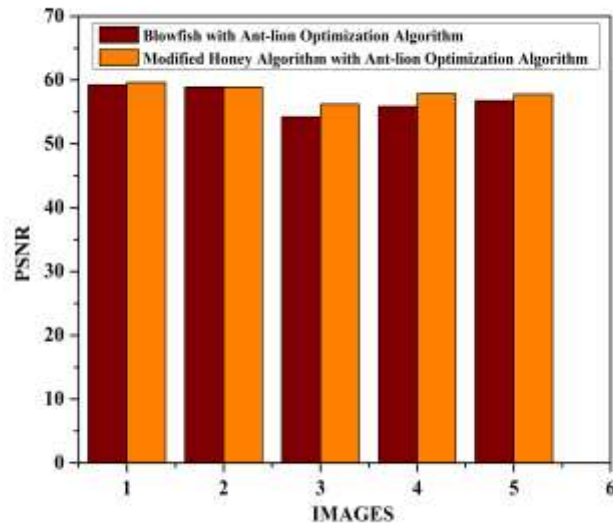


Figure 1: Peak Signal to Noise Ratio (PSNR)

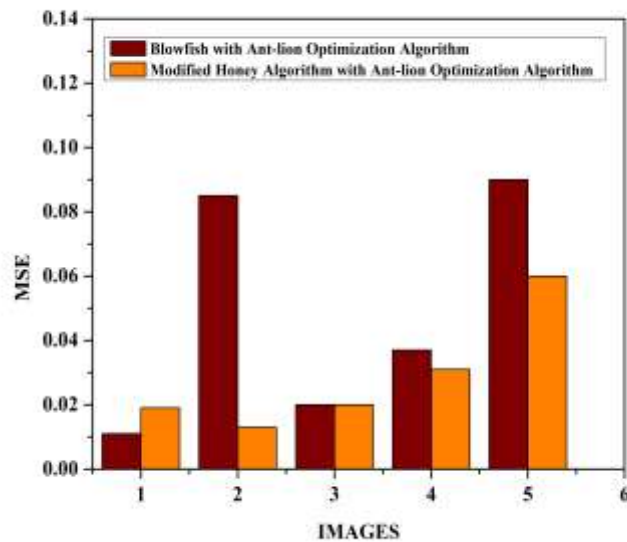


Figure 2 : Mean Square Error (MSE)

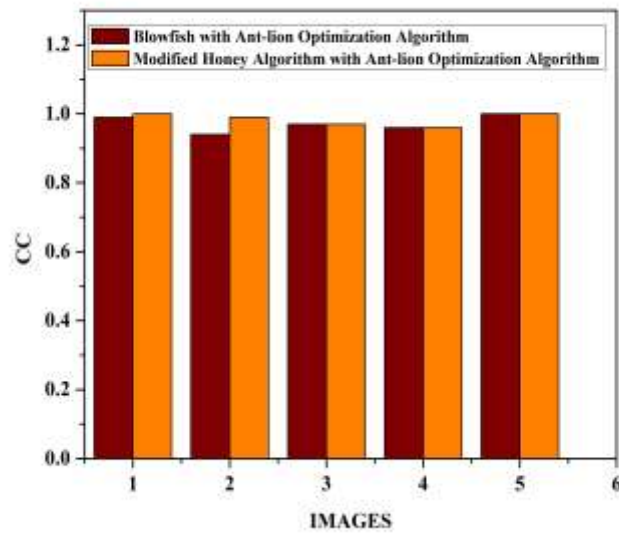


Figure 3: Correlation Coefficient (CC)

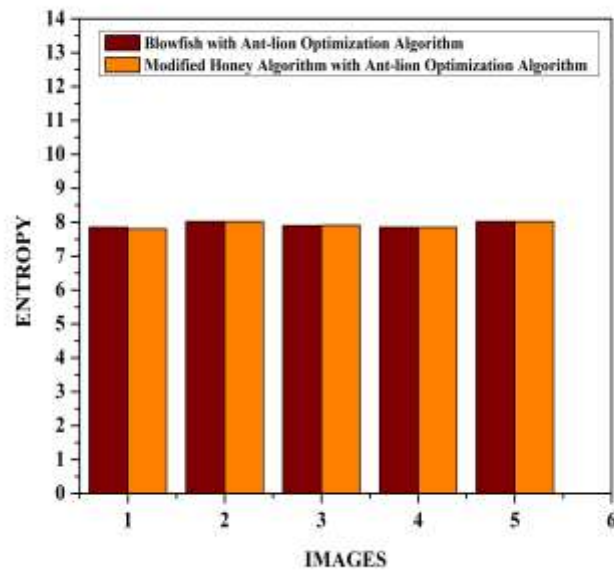


Figure 4: Entropy

V. PERFORMANCE MEASURE

The performance measures of Modified Honey Encryption with Ant-lion Optimization showed up in Table 1. The Modified Honey Encryption algorithms which transmit the medical image protected and secure way. The maximum estimation of the Peak signal to noise ratio in the proposed method is 59.93 as shown in table 2

Table 1 contains the other performance of Noise signal, Error, Correlation Coefficient and Entropy of other techniques, for instance, The Modified Honey encryption here exhibits the PSNR of different security calculations. Modified Honey are about the equivalent and don't change fundamentally. This affirms that the Modified honey encryption performs well for a wide scope of Medical images. The estimation of relationship coefficient in near unity. Mean square error is figured by determining the blunder bits over all bits in the medical image. The Mean Square Error regard for the HE is lower when appeared differently in relation to the next algorithm.

VI. STUDY RESULTS, SUMMARY AND CONTRIBUTION

Here this article the Modified Honey Encryption Algorithm is optimized with Ant-Lion optimizer. modified HE is used to extend the safety for medical imaging technique. Ant-Lion optimization both the keys are optimized during encryption process. Performances of the Modified Honey encryption technique which are raised and evaluated by Entropy, PSNR, CC and MSE. The entropy maximizes with Modified Honey Encryption model and the PSNR value seems to be high than the other. The computing effort and the necessary computation time will decrease with this Modified Honey encryption. We consider some medical images, And that medical image was collected from hospitals for security analysis. Security measures are examined by adding image encryption scheme.

VII. ACKNOWLEDGMENT

We would like to thank Kalasalingam Academy of Research and Education and also thank the Department of Electronics and Communication Engineering for permitting to use the computational facilities available in Digital Signal Processing Laboratory.

REFERENCES

1. T. Avudaiappan , R. Balasubramanian , S. Sundara Pandiyan, M. Saravanan, S. K. Lakshmanaprabu ,K. Shankar., Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm Journal of Medical Systems (2018) 42:208 ,2018
2. Annaby, M. H., Rushdi, M. A., and Nehary, E. A., Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion. Opt. Lasers Eng. 103:9–23, 2018.
3. k.shankar , mohamed elhoseny, e. dhiravida chelvi, s. k. lakshmanaprabu, wanqing wu., An Efficient Optimal Key Based Chaos Function for Medical Image Security. Digital Object Identifier, vol.6, pp 77145-77154, 2018
4. S. Guhan ,S. Arumugham ,S. Janakiraman A. Rengarajan S. Rajagopalan., A Trio Approach Satisfying CIA Triad for Medical Image Security. 2018

5. Abdulaziz shehab,mohamed elhoseny, khan muhammad,arun kumar sangaiah, po yang, haojun huang, and guolin hou., Secure and Robust Fragile Watermarking Scheme for Medical Images.Digital Object Identifier, 2018.
6. Zhongyun Hua,Shuang Yib,Yicong Zhou.,Medical image encryption using high-speed scrambling and pixel adaptive diffusion.2017
7. Padmapriya,Praveenkumar,N.KerthanaDevi ,Dhivya Ravichandran, J.Avila1, K. Thenmozhi, John Bosco Balaguru Rayappan1,Rengarajan,Amirtharajan.,Transreceiving of encrypted medical image – a cognitive approach.,2018
8. Ahmed, a. abd el-latif, Bassem abd-el-atty, muhammad talh., Robust Encryption of Quantum Medical Images.,2017
9. Ahmed a. abd el-latif, bassem abd-el-atty, m. shamim hossain md. abdur rahman atif alamri, b. b.gupta.,Efficient Quantum Information Hiding for Remote Medical Image Sharing,2018
10. 1Shankar K, Lakshmanaprabu S.K.,Optimal key based homomorphic encryption for color image Security aid of ant lion optimization algorithm, International Journal of Engineering & Technology, 7 (1.9) (2018) 22-27
11. Thakur,A. K. Singh,S.P.Ghrera,A.Mohan.,Chaotic based secure watermarking approach for medical images,Multimedia Tools and Applications, 2018.
12. Amiya Halder,AvranilMaity,Apurba Sarkar and Ananya Das.,A Dynamic Spatial Fuzzy C-Means Clustering-Based Medical Image Segmentation,2019
13. Samar M. Ismail, Lobna A. Saidb, Ahmed G,Radwan,Ahmed H,Madianb,Mohamed,F.Abu-Elyazeede. Generalized Double-Humped Logistic Map-based Medical Image Encryption,2018.
14. Lisha Ma1, Lei Chen,Shihong Wang., Security analysis of a reversible watermarking algorithm for encrypted images in wavelet domain, Multimedia Tools and Applications ,2018
15. Med Karim Abdmouleha, Ali Khalfallaha, Med Salim Bouhlela. A Novel Selective Encryption Scheme for Medical Images Transmission based-on JPEG Compression Algorithm, Procedia Computer Science 112 (2017) 369–376,2017
16. K. Shankar P. Eswaran.,RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique, Journal of Circuits, Systems, and Computer, 2016
17. Shankar K, Eswaran P.,Sharing a Secret Image with Encapsulated Shares in Visual Cryptography, Procedia Computer Science 70 (2015) 462 – 468, 2015
18. A.Kanso, M. Ghebleh. An efficient and robust image encryption scheme for medical Applications, Communication Nonlinear Sci Numeric Simulator 24 (2015) 98–116.
19. Maryam Jaberi, George Bebis, Muhammad Hussai, Ghulam Muhammad., Accurate and robust localization of duplicated region in copy–move image forgery, 2013
20. Shankar K, Lakshmana Prabu S. K, Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm, International Journal of Engineering & Technology, 2018.
21. Sharma, A., & Rai, A. (2019). Improved attribute based encryption scheme in cloud to representative authorization framework for EHR services. International Journal of Control and Automation, 12(6), 1-8. doi:10.33832/ijca.2019.12.6.01

22. Bhardwaj, A., Som, S., & Muttoo, S. K. (2019). Sponge function based authentication encryption technique (SAFE) using robust initialization vector and ChaCha stream cipher. *International Journal of Advanced Science and Technology*, 28(20), 568-579. Retrieved from www.scopus.com
23. Ernest Ravindran, R. S., Priyadarshini, K. M., Sai, A. T., Shiny, P., & Sabeena, S. (2019). Design of finite field multiplier for efficient data encryption. *International Journal of Advanced Science and Technology*, 28(20), 42-52. Retrieved from www.scopus.com
24. Jaswanth Kumar Reddy, R., Rene Beulah, J., & Nalini, M. (2020). Applying attribute - based encryption to eliminate duplicate copies of identical data in cloud. *Test Engineering and Management*, 82, 10579-10584. Retrieved from www.scopus.com
25. Ibraheem, I. N., Hassan, S. M., & Abeam, S. A. (2020). Comparative analysis & implementation of image encryption & decryption for mobile cloud security. *International Journal of Advanced Science and Technology*, 29(3 Special Issue), 109-121. Retrieved from www.scopus.com