RESEARCH ARTICLE OPEN ACCESS

Image Encryption and Decryption Using Signcryption

Balsing S
Government Arts College (Autonomus)
Kumbakonam-Thanjavur

ABSTRACT

The implementation of a system that combines encryption strategies to offer security to exchanged images is the main difficulty of this paper. The device is primarily based on a hybrid algorithm that applies the strategies of encryption and optimization techniques are used. This technique Signcryption is the technique that mixes the functionality of encryption and digital signature in a single logical step. From the implementation, the results are evaluated through the usage of the Peak Signal to Noise Ratio (PSNR) and Mean square errors (MSE).

Keywords: Image Security, Encryption, optimization and signcryption.

I. INTRODUCTION

The security of medical images which are stored on digital media is vital. These images might be extensive in size and number, and for the most part, contain private image [1]. As digital images are normally indicated by two dimensional, so as to quickly track de-connect relations among pixels [2], we execute a higher dimensional encryption key utilizing the decimal development of an irrational number and after that use it to rearrange the situation of pixels in the secret image [3-10]. Storage and transmission, encryption is an extremely [11] proficient device, yet once the sensitive information is decrypted, the data isn't ensured any longer [12]. If the images are in plain-text, then it is difficult to access it and of the day by day logs by the intruder. Most basic encryption algorithms put the accentuation on text data or paired data [13-14]. In this manner, the standard customary ciphers like IDEA, AES, DES, and RSA etc. are not proper for continuous image encryption as these ciphers needed high computational time and power for registering [8]. By understanding the advantages of encryption in giving a capable security to unique data, an effective algorithm is introduced to encrypt and decrypt the medical images [15-20]. The ideas of Optimization Algorithm are to scramble and decrypt the image for securely trading it between the transmissions as well as receiving side images [21-30]. This paper discussed the image security for the stored images with optimal signcryption technique. Here AEHO technique is presented to choose the optimal keys of encryption and decryption model.

II. LITERATURE REVIEW

In 2016 Shankar et al. [31] have proposed the n ECC method, the public key is randomly generated in the encryption process and decryption process, the private key (H) is generated by utilizing the optimization technique and for evaluating the performance of the optimization by using the PSNR. From the test results, the PSNR has been exposed to be 65.73057, also the mean square error (MSE) value is 0.017367 and the correlation coefficient (CC) is 1 for the decrypted image without any distortion of the original image and the optimal PSNR value is attained using the cuckoo search (CS) algorithm when compared with the existing works.

A sender transmits the secret image which is divided into shares and it holds hidden information by Shankar K et al.[32]. Have suggested these process, shares and AES algorithm binds together to give the resultant shares are called the encapsulated shares. Consequently, the secret image information cannot be retrieved from any one transparency via human visual perception.The Proposed scheme offers better security for shares and also reduces the fraudulent shares of the secret image. Further, the experimental results and analyses have demonstrated that the proposed scheme can effectively encrypt the image with the fast execution speed and minimized PSNR value.

The proposed study, Homomorphic Encryption (HE) with optimal key selection for image security is utilized by Shankar K et al.[33]. Here the histogram equalization is introduced for altering image intensities to improve contrast. The histogram of an image generally speaks to the comparative frequency of occurrence of the different graylevels in the image. To increase the security level inspired Ant Lion Optimization (ALO) is considered, where the fitness function as max entropy the best-encrypted image is characterized as the image with most astounding entropy among adjacent pixels. Analyzing the outcomes from the performed experimental outcomes can accomplish abnormal state and great strength of proposed model compared with other encryption strategies.

In 2017 Sathesh Kumar et al.[34] The distinctive encryption strategies are cloud sensitive data security process. On the off chance that the data owner stores the sensitive data to cloud server, the data owner is encrypted their data encryption systems. Here, AES, RSA, Blowfish and ECC encryption techniques are considered. From the security model, the most data secure in blowfish encryption contrasted with different procedures in view of encryption and decryption time with data.

In 2018 . Avudaiappan et al.[36] the dual encryption procedure is utilized to encrypt the medical images. Initially Blowfish Encryption is considered and then signcryption algorithm is utilized to confirm the encryption model. After that, the Opposition based Flower Pollination (OFP) is utilized to upgrade the private and public keys. The performance of the proposed strategy is evaluated using performance measures such as Peak Signal to Noise Ratio (PSNR), entropy, Mean Square Error (MSE), and Correlation Coefficient (CC) [37].

2. An Image Security Methodology

The main objective of this work is to develop a mutually authenticated image transmission protocol that provides confidentiality, integrity, and authenticity of the images. There are a few security issues related to digital medical image processing and transmission, so it is essential to keep up the uprightness as well as the secrecy of the image. Initially, the standard images are considered for security process that is encryption and decryption model, here AEHO based signcryption technique is proposed. The purpose of optimal key selection in security strategy is choosing optimal private and public key in both sender and receiver side. After the images encryption, it's stored in the cloud or relevant area, after that optimal private key is used for the image decryption process, here the optimal keys are attained based on the objective function as Maximum PSNR value and this proposed model is implemented in MATLAB platform [38-45].

2.1 Image Security using Signcryption Algorithm

A novel technique for public key cryptography is Signcryption which simultaneously satisfies both the elements of digital signature and open key encryption with lower cost. The properties included in signcryption are Confidentiality, Unforgeability, Integrity, and Non-repudiation. Some signcryption consists of additional attributed such as Public verifiability and forward secrecy of message confidentiality. This work consists of three models, for example, key generation, signcryption, and unsigncryption process.

2.1.1 Key Generation

The Signcryption, represents a public-key primitive which constitutes two vital cryptographic gadgets which are capable of ensuring the privacy, honesty, and non-repudiation. It simultaneously performs the tasks of both digital signature and encryption. This initialization process initializes the prime numbers, hash functions with keys. In light of these, we get the private and public key for both the sender and beneficiary. To improve the medical image security, the proposed technique utilizes the ideal private keys by the optimization process.

Initialization:-

L_P -Large prime number

L_f - Large prime factor

I - Integer with order L_f modulo L_P, chosen randomly from [1,… L_P -1]

Hash- One way hash function, whose output has at least 128 bits,

L_P - Keyed one way hash function

D - Value, chosen randomly [1,… L_f -1]

Sender Key pair ((M_{k1}, N_{k1}))

$$M_{k1} = Q^{A_{k1}} \bmod L_P \quad (1)$$

Receiver key pairs (M_{k2}, N_{k2})

$$N_{k2} = Q^{A_{k2}} \bmod L_P \quad (2)$$

2.1.2 Signcryption with Optimal keys

From the optimal keys, the image will be secured with the help of signcryption strategy. Signcryption is public key primitive that simultaneously executes the elements of both digital signature and encryption. With the expectation of assessing the hash value, uses the receiver public key. The detailed steps of this process mentioned in below section.

Steps:

- Select the sender values from the range of $(1 - L_f)$
- Evaluate the hash function of the sender utilizes the receiver optimal Public key (opt_Y_{k2}) ith the hash function and its deliver 128-bit plain image into two 64bit hash outputs.
  - $H_O = hash(N_{k2}{}^D \bmod P_{rn})$ (1)
- Then, he performs the encryption of the data with the assistance of the encryption (E) algorithm with OH$_1$. Thus, he gets hold of the sender cipher image (C_I) as illustrated in the following Equation.
  - $C_I = Enc\_H_{O1}(image)$ (2)
- Now, he effectively utilizes the H_{O2} value in the one-way keyed hash function KH to achieve a hash of the data, which leads to the 128-bit hash, labeled as U .
  - $U = L_p \, H_{O2}(image)$ (3)
- Finally, he evaluates the value S by means of Equation 11 shown hereunder.
  - $S_I = \dfrac{D}{(D + D_{O1H}) \bmod L_f}$ (4)
- Thus, the send pockets three distinct values such as $S_I, U \text{ and } C_I$ the, which are subsequently communicated to the receiver.

2.2.2 Unsigncryption

- The receiver end performs the function of decryption of the data by carrying out the successive steps in the unsigncryption phase.
- The sender effectively utilizes the values of $S_I, U \text{ and } C_I$ receiver private key, sender public key, P and G to estimate a hash which ultimately offers the 128-bit output.
  - $H_O = hash((N_{k1} * D^R)^s *^{M_{k2}} \bmod L_p)$ (5)
- The receiver consequently uses the key H_{O1} to decrypt the cipher text C$_t$, which eventually users in the data.
  - $Dec\_image = Dec\,H_{O1}(C_I)$ (6)
- Based on above signcryption and unsigncryption process based the images are secure the image. Recognize the legitimate message if. It goes to the subsequent stage which is the designcryption, implying the received image m is genuine.

III. RESULT AND ANALYSIS

This proposed image security model applied in MATLAB 2015a with an i5 processor and 4GB RAM. For this evaluation model, various images are taken into consideration such as Lena, cameramen baboon and pepper. Some of the performance measures are used they are PSNR, Mean square Error (MSE) values.

TABLE 1: Image Security Results

Images		Encrypted	Decrypted	PSNR	MSE
Lena				59.52	0.02

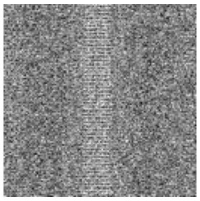
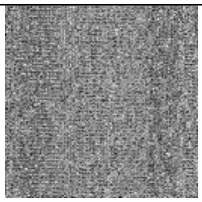
Cameramen				57.52	0.04
Baboon				56.22	0.08
pepper				55	0.11

Table 1 display that the image security results of a proposed technique that is the most beneficial sign cryption approach, the measures such as PSNR and MSE. At yield decryption algorithm related so as to procure precise image again. For this reason, twofold security is acquired through the transmission. After transmission, the bit is eliminated from it, to attain are a complete image. If the Lena image the most PSNR is 59.52dB and 0.05 MSE in the proposed version, further the outcomes are analyzed.

IV. CONCLUSION

In this paper analyzed the image security method with most excellent signcryption method's the encryption system, the non-public key and the general public key are optimized utilizing AEHO based signcryption approach. The performances of the proposed approach are evaluated by the usage of PSNR and MSE. In addition to these, there are several different problems exist consisting of total keys size as well as computation used in the previous algorithm may be very big. From the implementation consequences the most PSNR is 56.22dB and minimal MSE is zero.22.Therefore the confidentiality of the image is upheld ultimately and the reclaimed image is obtainable the particular image without in any way adversely influencing the quality of the image.

In the future scope, the hybrid optimization model is taken into consideration to the growing level of the image.

REFERENCE

[1] Chen, Y. T., Chen, C. H., Wu, S., & Lo, C. C. (2019). A two-step approach for classifying music genre on the strength of AHP weighted musical features. Mathematics, 7(1), 19.

[2] Elhoseny, M., Shankar, K., &Uthayakumar, J. (2019). Intelligent diagnostic prediction and classification system for chronic kidney disease. Scientific reports, 9(1), 1-14.

[3] Sivakumar, P., Velmurugan, S. P., & Sampson, J. (2020). Implementation of differential evolution algorithm to perform image fusion for identifying brain tumor.

[4] Khamparia, A., Gupta, D., Nguyen, N. G., Khanna, A., Pandey, B., & Tiwari, P. (2019). Sound classification using convolutional neural network and tensor deep stacking network. IEEE Access, 7, 7717-7727.

[5] 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.

[6] Jain, R., Gupta, D., & Khanna, A. (2019). Usability feature optimization using MWOA. In International

conference on innovative computing and communications (pp. 453-462). Springer, Singapore.

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

[8] Lyu, L., & Chen, C. H. (2020, July). Differentially Private Knowledge Distillation for Mobile Analytics. In Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (pp. 1809-1812).

[9] Poonkuntran, S., Rajesh, R. S., & Eswaran, P. (2011). Analysis of difference expanding method for medical image watermarking. In International Symposium on Computing, Communication, and Control (ISCCC 2009) (Vol. 1, pp. 31-34).

[10] Sampson, J., & Velmurugan, S. P. (2020, March). Analysis of GAA SNTFT with Different Dielectric Materials. In 2020 5th International Conference on Devices, Circuits and Systems (ICDCS) (pp. 283-285). IEEE.

[11] Elhoseny, M., Bian, G. B., Lakshmanaprabu, S. K., Shankar, K., Singh, A. K., & Wu, W. (2019). Effective features to classify ovarian cancer data in internet of medical things. Computer Networks, 159, 147-156.

[12] Gochhayat, S. P., Kaliyar, P., Conti, M., Tiwari, P., Prasath, V. B. S., Gupta, D., & Khanna, A. (2019). LISA: Lightweight context-aware IoT service architecture. Journal of cleaner production, 212, 1345-1356.

[13] Dutta, A. K., Elhoseny, M., Dahiya, V., & Shankar, K. (2020). An efficient hierarchical clustering protocol for multihop Internet of vehicles communication. Transactions on Emerging Telecommunications Technologies, 31(5), e3690.

[14] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, BioSenHealth 1.0: A Novel Internet of Medical Things (IoMT) Based Patient Health Monitoring System, Lecture Notes in Networks and Systems. Springer, 2019

[15] Shankar, K., Lakshmanaprabu, S. K., Khanna, A., Tanwar, S., Rodrigues, J. J., & Roy, N. R. (2019). Alzheimer detection using Group Grey Wolf Optimization based features with convolutional classifier. Computers & Electrical Engineering, 77, 230-243.

[16] Paramathma, M. K., Pravin, A. C., Rajarajan, R., & Velmurugan, S. P. (2019, April). Development and Implementation of Efficient Water and Energy Management System for Indian Villages. In 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS) (pp. 1-4). IEEE.

[17] Chen, C. H., Song, F., Hwang, F. J., & Wu, L. (2020). A probability density function generator based on neural networks. Physica A: Statistical Mechanics and its Applications, 541, 123344.

[18] Kathiresan, S., Sait, A. R. W., Gupta, D., Lakshmanaprabu, S. K., Khanna, A., & Pandey, H. M. (2020). Automated detection and classification of fundus diabetic retinopathy images using synergic deep learning model. Pattern Recognition Letters.

[19] Gupta, D., & Ahlawat, A. K. (2016). Usability determination using multistage fuzzy system. Procedia Comput Sci, 78, 263-270.

[20] Amira S. Ashour, Samsad Beagum, Nilanjan Dey, Ahmed S. Ashour, Dimitra Sifaki Pistolla, Gia Nhu Nguyen, Dac-Nhuong Le, Fuqian Shi (2018), Light Microscopy Image De-noising using Optimized LPA-ICI Filter, Neural Computing and Applications, Vol.29(12), pp 1517–1533, Springer, ISSN: 0941-0643. (SCIE IF 4.664, Q1)

[21] Pan, M., Liu, Y., Cao, J., Li, Y., Li, C., & Chen, C. H. (2020). Visual Recognition Based on Deep Learning for Navigation Mark Classification. IEEE Access, 8, 32767-32775.

[22] Chen, C. H., Hwang, F. J., & Kung, H. Y. (2019). Travel time prediction system based on data clustering for waste collection vehicles. IEICE TRANSACTIONS on Information and Systems, 102(7), 1374-1383.

[23] Shankar, K., & Eswaran, P. (2015). ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm. Int J Appl Eng Res, 10(55), 1841-5.

[24] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, Dac Nhuong Le, Smart Surveillance Robot for the Real Time Monitoring and Control System in Environment and Industrial Applications, Advances in Intelligent System and Computing, pp 229-243, Springer

[25] Le Nguyen Bao, Dac-Nhuong Le, Gia Nhu Nguyen, Vikrant Bhateja, Suresh Chandra Satapathy (2017), Optimizing Feature Selection in Video-based Recognition using Max-Min Ant System for the Online Video Contextual Advertisement User-Oriented System, Journal of Computational Science,

Elsevier ISSN: 1877-7503. Vol.21, pp.361-370. (SCIE IF 2.502, Q1)

[26] Chakchai So-In, Tri Gia Nguyen, Gia Nhu Nguyen: Barrier Coverage Deployment Algorithms for Mobile Sensor Networks. Journal of Internet Technology 12/2017; 18(7):1689-1699.

[27] Le, D.-N.a, Kumar, R.b, Nguyen, G.N., Chatterjee, J.M.d, Cloud Computing and Virtualization, DOI: 10.1002/9781119488149, Wiley.

[28] Bhateja, V., Gautam, A., Tiwari, A., Nhu, N.G., Le, D.-N, Haralick features-based classification of mammograms using SVM, Advances in Intelligent Systems and Computing, Volume 672, 2018, Pages 787-795.

[29] Khamparia, A., Saini, G., Gupta, D., Khanna, A., Tiwari, S., & de Albuquerque, V. H. C. (2020). Seasonal crops disease prediction and classification using deep convolutional encoder network. Circuits, Systems, and Signal Processing, 39(2), 818-836.

[30] Uthayakumar, J., Elhoseny, M., & Shankar, K. (2020). Highly Reliable and Low-Complexity Image Compression Scheme Using Neighborhood Correlation Sequence Algorithm in WSN. IEEE Transactions on Reliability.

[31] Huyen, D.T.T., Binh, N.T., Tuan, T.M., Nguyen, G.N, Dey, N., Son, L.H, Analyzing trends in hospital-cost payments of patients using ARIMA and GIS: Case study at the Hanoi Medical University Hospital, Vietnam, Journal of Medical Imaging and Health Informatics, 7(2), pp. 421-429.

[32] Van, V.N., Chi, L.M., Long, N.Q., Nguyen, G.N., Le, D.-N, A performance analysis of openstack open-source solution for IaaS cloud computing, Advances in Intelligent Systems and Computing, 380, pp. 141-150.

[33] Shankar, K., & Eswaran, P. (2016, January). A new k out of n secret image sharing scheme in visual cryptography. In 2016 10th International Conference on Intelligent Systems and Control (ISCO) (pp. 1-6). IEEE.

[34] Dey, N., Ashour, A.S., Chakraborty, S., Le, D.-N., Nguyen, G.N, Healthy and unhealthy rat hippocampus cells classification: A neural based automated system for Alzheimer disease classification, Journal of Advanced Microscopy Research, 11(1), pp. 1-10

[35] Velmurugan, S. P., & Rajasekaran, P. S. M. P. (2017). CLASSIFICATION OF BRAIN TUMOR USING MULTIMODAL FUSED IMAGES AND PNN. International Journal of Pure and Applied Mathematics, 115(6), 447-457.

[36] Shankar, K., Elhoseny, M., Perumal, E., Ilayaraja, M., & Kumar, K. S. (2019). An Efficient Image Encryption Scheme Based on Signcryption Technique with Adaptive Elephant Herding Optimization. In Cybersecurity and Secure Information Systems (pp. 31-42). Springer, Cham.

[37] Wu, L., Chen, C. H., & Zhang, Q. (2019). A mobile positioning method based on deep learning techniques. Electronics, 8(1), 59.

[38] Lydia, E. L., Kumar, P. K., Shankar, K., Lakshmanaprabu, S. K., Vidhyavathi, R. M., & Maseleno, A. (2020). Charismatic document clustering through novel K-Means non-negative matrix factorization (KNMF) algorithm using key phrase extraction. International Journal of Parallel Programming, 48(3), 496-514.

[39] Sujitha, B., Parvathy, V. S., Lydia, E. L., Rani, P., Polkowski, Z., & Shankar, K. (2020). Optimal deep learning based image compression technique for data transmission on industrial Internet of things applications. Transactions on Emerging Telecommunications Technologies, e3976.

[40] Lo, C. L., Chen, C. H., Hu, J. L., Lo, K. R., & Cho, H. J. (2019). A fuel-efficient route plan method based on game theory. Journal of Internet Technology, 20(3), 925-932.

[41] Kung, H. Y., Chen, C. H., Lin, M. H., & Wu, T. Y. (2019). Design of Seamless Handoff Control Based on Vehicular Streaming Communications. Journal of Internet Technology, 20(7), 2083-2097.

[42] Elhoseny, M., & Shankar, K. (2019). Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Transactions on Reliability.

[43] Shanmugam, P., Rajesh, R. S., & Perumal, E. (2008, May). A reversible watermarking with low warping: an application to digital fundus image. In 2008 International Conference on Computer and Communication Engineering (pp. 472-477). IEEE.

[44] Shankar, K., & Elhoseny, M. (2019). Trust Based Cluster Head Election of Secure Message Transmission in MANET Using Multi Secure Protocol with TDES. J. UCS, 25(10), 1221-1239.

[45] Parvathy, V. S., Pothiraj, S., & Sampson, J. (2020). Optimal Deep Neural Network model based multimodality fused medical image classification. Physical Communication, 101119.

[46] Subbiah Parvathy, V., Pothiraj, S., & Sampson, J. (2020). A novel approach in multimodality medical

image fusion using optimal shearlet and deep learning. International Journal of Imaging Systems and Technology.

[47] Parvathy, V. S., & Pothiraj, S. (2019). Multi-modality medical image fusion using hybridization of binary crow search optimization. Health Care Management Science, 1-9.

[48] Velmurugan, S. P., Sivakumar, P., & Rajasekaran, M. P. (2018). Multimodality image fusion using centre-based genetic algorithm and fuzzy logic. International Journal of Biomedical Engineering and Technology, 28(4), 322-348.

[49] Chen, C. H. (2018). An arrival time prediction method for bus system. IEEE Internet of Things Journal, 5(5), 4231-4232.

[50] Shankar, K., Perumal, E., & Vidhyavathi, R. M. (2020). Deep neural network with moth search optimization algorithm based detection and classification of diabetic retinopathy images. SN Applied Sciences, 2(4), 1-10.

[51] Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. Future Generation Computer Systems, 102, 1027-1037.

[52] Elhoseny, M., & Shankar, K. (2020). Energy efficient optimal routing for communication in VANETs via clustering model. In Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks (pp. 1-14). Springer, Cham.

[53] Chen, C. H. (2020). A cell probe-based method for vehicle speed estimation. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 103(1), 265-267.

[54] Khamparia, A., Singh, A., Anand, D., Gupta, D., Khanna, A., Kumar, N. A., & Tan, J. (2018). A novel deep learning-based multi-model ensemble method for the prediction of neuromuscular disorders. Neural computing and applications, 1-13.

[55] Shankar, K., Zhang, Y., Liu, Y., Wu, L., & Chen, C. H. (2020). Hyperparameter tuning deep learning for diabetic retinopathy fundus image classification. IEEE Access, 8, 118164-118173.