WSN-based cryptography techniques to avoid misuse of the patient reports communication between patient and hospital

[1]K Muthulakshmi and [2]T. Jaya Sankar
[1]Professor/ Electronics and Communication Engineering,
Sri Krishna College of Technology, Coimbatore
kavi.neha@gmail.com
[2]Assistant Professor (Sr. Gr)
Department of Electronics and Communication Engineering,
University College of Engineering
BIT Campus, Anna University, Tiruchirappalli.
jayasankar27681@gmail.com

Abstract

In this work, we propose and implement a secure communication method that combines compression, user authentication, and decryption. In terms of transmitting medical images, the suggested approach offers an improvement over the current methods. Therefore, We present a novel encrypted transmission technique that uses smart agents to communicate and make decisions in order to do tasks like SVD compression, digital signature-based user authentication, AES and RSA picture encryption, and Hill-Cipher data encryption. Images delivered either with an embedded message or on their own are encrypted using one of two different methods to increase security. Decisions on the sort of encryption to be performed are determined using rules, with consideration given to both the nature of the material and the intended recipients. Sender and receiver sides of unicast communications employ the MAES algorithm and 128-bit key for encryption and decryption, respectively. Experiments were undertaken to evaluate the suggested model, and the results showed improvements in transmission speed, security, compression/decompression efficiency, and the ability to make informed decisions about sending medical images.

Keyword: cryptography, secured transmission, Wireless Sensor Network, authentication, embedded message and ElGamal cryptography.
DOI Number: 10.14704/nq.2022.20.11.NQ66173 **NeuroQuantology 2022; 20(11): 1782-1793**

1. Introduction

Wireless Sensor Network (WSN) is an important and useful contribution among the various innovations provided by researchers for the enhancement of networking technologies in the future. The WSN is upgraded by the presentation of developments in the field of information openness, monetary and brilliant sensors that can bring the efficient deployment of sensor hubs in the sensing field. Low-cost, low-power, multipurpose sensor that are compact and can communicateover short distances have become possible because to wireless communications and digital electronics [1]. The concept of sensor networks, which relies on the combined efforts of many individual nodes, is influenced by these miniature sensor nodes, which include sensing, data processing, mechanisms.These sensor nodes are dispensed spatially and it works cooperatively in nature for imparting the information collected from the monitored area through remote connections. The data grouped many sensor nodes are communicated to the destination node that whether it uses the data locally is related to other sensor networks. The WSN technology provides different kinds of features on different networking solutions, in particular, the arrangement of unwavering quality [2], lower costs, exactness, versatility, adaptability, and simple to upgrade the associations which are used to enhance the usage of assorted application environment monitoring, military communications, information security and healthcare system.

In sensor networks, every sensor node consists of sensing devices that are consuming less power with the incorporated processor, power module and communication channel. Generally, the embedded processor is used to

eISSN 1303-5150

gather and handle the signal data from sensors. In addition, all these kinds of sensor nodes are armed with reserved resources [3]. The sensor provides a quantitative response to a change over the physical situation like humidity, temperature and so on. In WSN,The wireless sensor nodes are used to restrict the range of data transmission and limited battery energy and the lifetime of a system is an important issue when designing any type of WSN application. The energy provided by the sensor node is put to good use here, lengthening the lifespan of the network as a whole. Energy-efficient data transmission from sensor nodes is a critical design challenge for ensuring the integrity of data in such a network. As a result of increased congestion, delay, and energy consumption, security attacks against such sensor nodes and the networks linking them would degrade the performance of network communication. The network's throughput will drop because of the lowered packet delivery ratio [4]. For this reason, it is important to provide effective methods of data collecting and secure methods of data distribution. When using a conventional cryptography system, the transmitter and the receiver both have their own unique sets of keysgenerated by distinct variables. Diffie-Hellman is a key exchange method that uses a distinct key exchange scheme despite the fact that public keys are utilised to simplify the key management process and provide increased security. With the use of a data concealing technique, encrypted information is concealed within a picture in steganography. Every business needs cryptography for data security because it keeps sensitive information private and prevents unauthorised access. People no longer have faith that passwords are able to guarantee reliability for their data because any cracker or invader may easily guess a password within a short amount of time. In spite which includes the Diffie-Hellman Algorithm, RSA, and the Digital Signature Algorithm, was developed in response to the need for stronger encryption. These cryptographic techniques, for example, were developed to counteract DoS attacks. Steganography relies heavily on the science of picture encryption and decoding. Confidential details are safely sent from sender to receiver by being encoded inside the photos themselves. In the context of combining steganography with cryptography, encryption refers to the process of using an encryption algorithm to transform the plaintext that will be hidden in a picture into the encrypted data known as Ciphertext. Numerous algorithms catering to the needs of data owners may be found in the relevant literature. Additionally, the normal encryption system is protected effectively with these combined methods [6]. There are a number of different decryption methods that may be used in this way to suit the needs of the data. These are also helpful for safeguarding data that has been encrypted using the standard encryption. The picture decryption procedure in this case is a method that converts an undecipherable cypher image into a recognisable plain image (original image). Additionally, these methods are made available throughout the decoding process, which transforms the cypher picture into a plain image by applying the algorithm and key, all without any loss of data or image features. This study encrypts and decrypts data using newly developed cryptographic techniques to ensure its safety [7].

2. Literature Survey

Literature deals with different variability records of work done by researchers in thetrack of WSN, Steganography, Cryptography, encryption and decryption techniques,Digital Signature and Secure Routing in WSNs.

Weiqi et al. [8] enhanced and improvised the existing Least Significant Bit whichis used for matching processed image which is revisited and also proposed a new edgeincorporated method is used to choose the best regions that are embedded accordingto the secret image size and find the pixels differences in a cover image. They haveused images for evaluation with particular steganalysis algorithms that are universal thatenhanced the security significantly when compared with typical LSB oriented schemesare very easy to execute and implement to get results in stego-images that containsembedded data as a hidden message. It is based on pixel-value-difference. This methodis reviewed and followed to preserve the high-quality visualization of the stego images.

eISSN 1303-5150

Xiao [9] developed and reconstitute a new methodology for reducing the volume of data transmission and resisting the different types of attackers in this work. Intheir work, they gave focused on the image multi-fusion according to the algorithmdecomposition of the wavelet for generating the complete images and also optimizingthe human eye perception. Moreover, their fused multi-focused images represent witha structure-based random matrix which reduced the voluminous of data with the initiallevel encryption process. In addition, their gained measurement values were encryptedfor resisting the data noise and also identifying the attacks by combining the permutation and the diffusion levels. Finally, they have reconstructed the decrypted in theirwork and it also demonstrated that the data security level and the robustness of theproposed methodology.

Wei [10] proposed an authentication scheme which is a blend that works according to the secret-sharing method with the capability of repair the data for color imageseither it may gray-scale documented images. Moreover, a recognized signal has created for every area of a gray-scale image that combined together with the binarized datawhich transformed into the various numbers of shares by applying the Shamir secretsharing method

lexey G and Anton A [11] initiated in their work process and analyzed the current trends in the security of WSNs that show that the most challenging issue of keymanagement. They also considered the issues and scope of key management to perform an encryption process on WSN. Finally, they introduced a hybrid key managementtechnique that uses the routing data that determines to perform the routing techniquesand the sensor network structure

Zhili et al. [12] distinguish between the processes of a novel substation orientedlinguistic-based steganalysis method according to the context clusters. They have introduced a new context cluster for estimating the fitness of context and also demonstratedthat the way of using the statistics over the context fitness values for distinguishes between the normal and stego texts. Lastly, they have achieved 98.86% as steganalysisaccuracy by conducting various experiments in their work.

Amir Hossein and Jalil Seifali[13] extended and developed with algorithms onsecret data. The network steganography concept to utilize the overlay cognitive radionetworks with systematic channel codes. They also proposed an approach in this direction which is embedding the cognitive and secret data from the transformed form intocodes.

Javaid A et al. [14] proposed a new data hiding technique which has highlycapable and reversible for embedding the medical images securely using the optimalpixel repetition method and it is converted into pixels as a 2 X 2 block with differentvalues. Moreover, the histogram invariance that enhances the heftiness of the projected method for handling the statistical attacks that is available. Finally, their methodachieved better performance and shows the efficiency in terms of preventing unauthorized access to secret data of clients.

Mao [15] developed a method for finding the leader by applying a lookup table-based approach. Their method is suitable to perform the embedding process over thesteganographic images based on linear and hamming code techniques. In their method,the closet syndrome has been applied for performing a search operation for the cossetleader over the standard error correction code. They have enhanced their method toperform the parity checking process which is used for making the syndrome that in-dictates that the cosset leader by itself. In their work, the size of the table is reducedsignificantly and the computational complexity.

Wei [16] proposed an authentication scheme which is a blend that works according to the secret-sharing method with the

eISSN 1303-5150

capability of repair the data for color imageseither it may gray-scale documented images. Moreover, a recognized signal has created for every area of a gray-scale image that combined together with the binarized datawhich transformed into the various numbers of shares by applying the Shamir secretsharing method.

Guanglou et al. [17] initiated then developed a framework and practically testedthe data with new novel methods. A critical analysis and also discussed the advantagesand disadvantages that are identified through the analysis in the setting of the ECG-based key distribution. Moreover, they have analyzed the major issues within eachand every key distribution technique that works based on primitives that include thegeneration and computation of binary and polynomial numbers. In addition, they alsodemonstrated that the method betterment based on false accepts and reject rates.

3. Proposed system

Four different algorithms are proposed. The first is the Elliptic Curve ElGamal cryptography for efficient data hiding; the second is the digital signature based Key generation and Verification Model; the third is the Binary Images for Secured Communiqué; and the fourth is the image Encryption for Secure data communication system architecture. For WSN, it is advised to use a new secure data communication paradigm that makes use of cryptographic procedures. There are ten primary mechanisms at work in the design. User interface image encryption and decryption, singular value decomposition, routing, and an energy management are some of these features. The 10 essential mechanisms need to be defined succinctly. We have been able to plan for and implement secure image transmission in WSN.

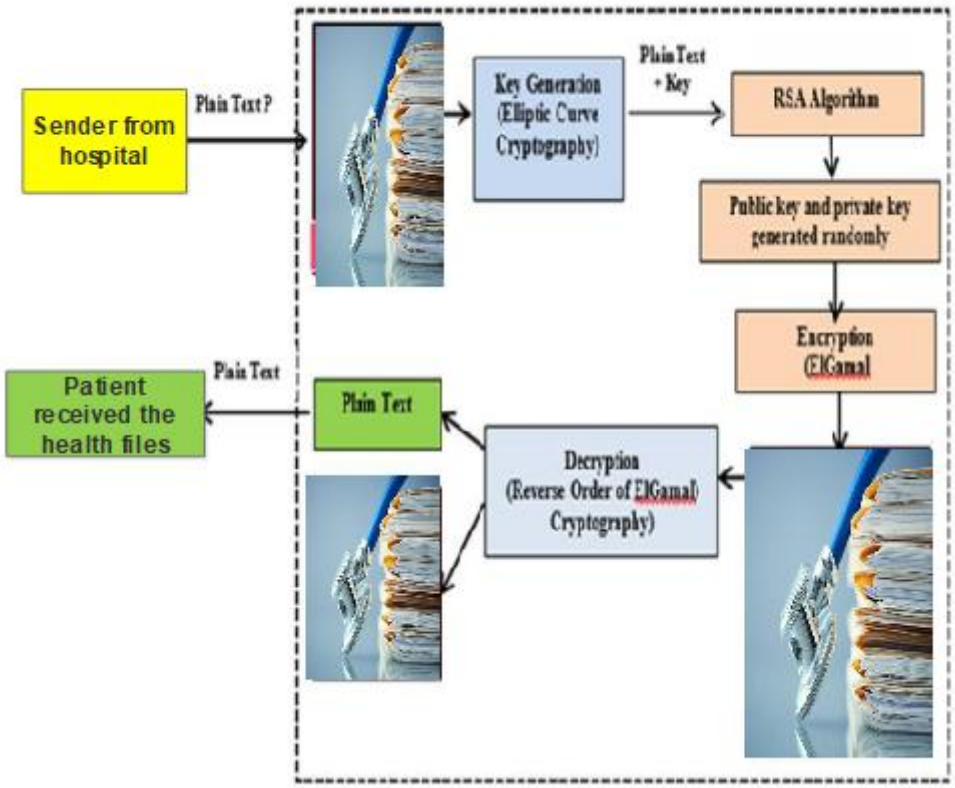


Figure. 1: Encrypted image-based hiding system architecture

eISSN 1303-5150

3.1 Proposed authentication and communication algorithms

Within the scope of this investigation, two methods are proposed for use in authentication and communication. All the computers in the experimental network follow rules that aid in authentication, encryption, and decryption, and the agents that aid in communication and coordination are also deployed on all the computers. Authentication, encryption, decryption, and message concealment via Hill-Cipher and embedding are the three components that make up each of these algorithms.

3.2 Cryptography

Cryptography is a technique of defensive data from prying eyes. Encryption methods and keys are the two mainstays of cryptography. In this case, the encryption process makes use of a number of different keys, each of which is optimal for the particular algorithm being employed. In this respect, a number of algorithms, such as DES, AES, TDES, and RSA, are at your disposal. There are two main types of cryptographic algorithms: those that rely on a symmetric key and those that rely on an asymmetric key. Similar to key-value encryption and decryption, the key value is put to use in symmetric key-based cryptography

3.3 Data hiding procedure

If the key is known or the key size is short enough, encrypted photos can be decrypted. For this reason, numerous scholars have proposed methods for encrypting images by first arranging their pixels into larger blocks. Although these techniques increased complexity, they did improve security.

$$y2 \equiv x3 + 4x + 4(mod\ 2773)$$

3.4 Elliptic curve Elgamal scheme

As part of this study, we employ a encryption system based on ElGamal cryptography and implemented using elliptic curves. Therefore, the following procedures make up the encryption system. Message in plaintext (P): input

Output: Ciphertext Posts C1 and C2

Phase 1: Choice a large prime sum p of 512 bits and read plaintext P and image I.

Phase 2: Reflect the elliptic curve $y2 = (x3 + ax + b)\ and\ find\ (x3 + ax + b)\ mod\ p$.

Phase 3: Discovery two points *'a' and 'b'* from the curve.

Phase 4: Deliberate the group $G =< Z * p, X >$ and excellentaassociate d from the collectionsuch that 1 <= d <= p − 2 and d = a selected from the elliptic curve.

Phase 5: Excellent e1 such that e1 is a rude root in group G.

Phase 6: Calculate$e2 = ed\ 1\ mod\ p$.

Phase 7: Make (e1, e2, p) as the public key and d as the secluded key for the receiver.

eISSN 1303-5150

Phase 8: Securely communicate the private key to the receiver.

Phase 9: At the sender cross, choice a random digit r from the group G.

Phase 10: Put on encryption cryptography as shadows:

Calculate C1 = er1 mod p and compute $C2 = (er\ 2 * P)$ mod p for cover imageseparately and message distinctly to get C1, C2 for embedded message andC3, C4 for the cover image using similar steps (2 to 10).

Phase 11: Send $C1, C2, C3\ and\ C4$ to the receiver.

Phase 12: At the receiver lateral, read $C1, C2, C3\ and\ C4$.

Phase 13: Compute $P = [C2 * (Cd\ 1) - 1]\ mod\ p\ and\ I = [C4 * (Cd\ 3) - 1]\ mod\ p$

Phase 14: In this approach, the picture I and the message P are kept apart, and then encrypted using the ElGamal encryption scheme based on elliptic curves to increase security. In order to increase security and decrease computing complexity, this work utilised the difference technique and performed data in groups. And the ElGamal encryption algorithm uses the q (1771, 705), from the polynomial y2 = (x3 + axe + b) that is utilised to represent the Elliptic curve.

$$y2 \equiv x3 + 4x + 4(mod\ 2773)$$

Sender wishes to send encrypted image I with message m attached. Elliptic curves and the ElGamal signature system were utilised to securely communicate between the sender and recipient.

$$y2 = (x3 + ax + b)$$

Here, the sender chooses an elliptic curve point p(a,b) and a huge prime, such as 2773, which we use to test our procedure. The sum of points on an elliptic curve is determined by the parameter p. A second number,, is selected by the sender, and q is then calculated using this value and the previous one, p. Here, both the sender and the receiver select and make public their respective points of interest (p and q). Here, we employ ElGamal-based encryption and decryption techniques for the encoding and decoding processes.

Expanding on the current Elliptic Curve based ElGamal Encryption Strategy, this thesis suggests a novel public-key encryption scheme in which the polynomial is chosen to represent the curve from whence the first two numbers are chosen to be used in the ElGamal encryption scheme.in order to deal with the difficulties presented by the existing techniques. The encryption and decryption methods used in this study make use of the elliptic curve points p = (1,3) and q = (1771, 705). There are a number of key distinctions between the proposed scheme and the alternatives already in use. The Elliptic curve points are selected first. Second, it generates keys and encrypts data using the ElGamal cryptosystem. Third, a random value is determined by taking the GCD of the two numbers. Finally, it employs the alternative approaches where double difference is considered rather than the single difference employed by conventional schemes. Thus, the suggested approach provides better security

eISSN 1303-5150

with less complexity than the existing arrangements that employ RSA-based public key procedures for key generation,. To further emphasise the visual aspect of the communication conveyed over the internet, the suggested model is also rescindable, so the recipient can decrypt both the en-crypted and encrypted versions.

3.5 Binary image encryption on vector space modelling for secured communication

The LEACH algorithm is improved in this investigation to provide a secure routing algorithm. In the past, many potential secure routing algorithms were conceived by combining the LEACH procedure with trust organization methods, key group and delivery methods, and intrusion detection procedures. However, most of the currently available methods cannot prevent attacks that modify or intercept data. This suggestion anticipates a new secured routing technique to address this issue by breaking down the image and messages into smaller parts, representing them in a matrix format, and then combining them to create an encrypted steganographic image based on rules established in this study. In addition, software agents known as intelligent communication agents have been deployed in all the sensor nodes present in the WSN to more reliably transmit the encrypted images to the neighbouring nodes.

User interface module

The user interface module acts as an intermediator between the decision manager andthe sensor nodes. The user interface module is used to transmit the data securely byapplying the proposed secured data communication model through a decision manager.The decision manager communicates with the user interface module for retrieving thedata and transmitting the data securely.

4. Results and discussion

For the purpose of measuring effectiveness, the proposed model has been put into action. Multiple experiments have been conducted to assess the efficacy of the proposed data hiding approach, with variables like image quality and payload taken into account. For this, we've tapped into the USC-SIPI image database and used it to demonstrate the quality gap between traditional approaches and our own, as well as the savings in data storage space that our approach offers. To begin, we have looked at the formula for calculating capacity as shown in Eqn. UCI's medical picture archive, which has 500 images, was used to evaluate this study. Java was used to create the working code for the algorithms, and Java Sockets were used for the communication. Java and Aglet-based mobile agents were employed for rule-based, efficient network communication between nodes.

Table 1: Simulation restrictions

Parameter	Value
Sum of Sensor Nodes	50 - 300
Energy of Nodes	2 J
Area (metre2)	200 m x 200 m
Initial Energy	0.5 J
Mobility Typical	Random Way Mobility
Mobility Speed	10 m/s to 50 m/s

The proposed secure Network Simulator. Table 1 shows the network parameters arelisted. In that table, a 250 X 250-meter square area was used to carry out the experiments. Also, reflect all the nodes that are energy of 2 Joules.

eISSN 1303-5150

Table 2: Encryption quality and runtime assessmentarrangement

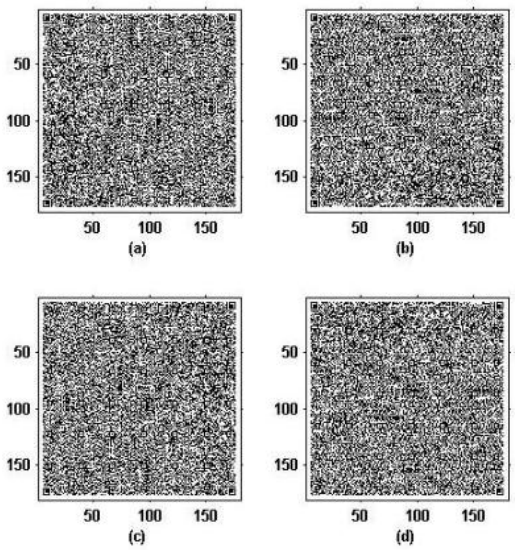
S.no	Reference	Normalized Correlation	PSNR, dB	Encryption time, s	Decryption time, s
1	[18]	0.0081	11.1309	811.7	861.1
2	Proposed methodology	0.0087	11.997	345.2	425.6

When compared to other methods in Table 2, it is clear that the optional encryption algorithm performs admirably. This is because authentication and encryption algorithms that are widely used..

Table 3: Illustrates the correlation values gotfor besmirched QR code

Variance	Speckle noise (CC)	Gaussian noise (CC)	Successfully retrieved cipher text
0.07	0.9795	0.9936	yes
0.10	0.9628	0.9917	yes
0.5	0.7926	0.9532	No
0.9	0.7405	0.8272	No

where E is the anticipation value. The Correlation Coefficient (CC) fordifferent variance values between the original and corrupt QR code iscalculated and it is shown in Table 3.



eISSN 1303-5150

Figures 2: (a)-(d) Shows encrypted QR code with degree rotation

It is important that a QR code be readable from any angle, thus we test the data container's readability by rotating it in different ways. Using a rotational analysis, a conventional reader can better ascertain the proper orientation of data containers that use QR-code functionality patterns. The position detection pattern ensures high-speed reading from any angle and guides the reader to the right QR code. All four possible QR code orientations (0, 90, 180, and 270 degrees) are shown in Figures 2 (a)-(d). Because QR codes can be read from any angle, the scanner can get all the information it contains.

Table 4:A correlation coefficient of images

Image		Horizontal	Vertical	Diagonal
CT Scan image	Plain	0.9815	0.9862	0.9834
	Cipher	-3.83	0.9852	-0.6798
X-ray images	Plain	0.978	0.8745	0.9781
	Cipher	6.198	0.5689	-0.015
MRI Scans images	Plain	0.971	0.8532	0.9876
	Cipher	0965	0.0021	-0.004113

This simulation demonstrates that the cypher image has a low pixel correlation distribution in the horizontal, vertical, and diagonal directions. Table 4 displays the correlation coefficients of the plain and cypher images, where it can be seen that the correction between neighbouring pixels is severely disrupted.

Table 5: Shows average execution time

Reference	Execution Time (s)
[19]	95.50
[20]	41.12
[21]	44.93
[22]	9.56
Proposed methodology	23

The work described here utilises MATLAB R2012a, 4 GB of RAM, 500 GB of hard disc space, and an Intel core i3 2.40 GHz CPU running on a Windows 7 operating system platform to demonstrate a colour picture cryptography technique. The proposed cryptography scheme takes an average of 24 seconds to run, with the classic approach having the fastest average calculation time compared to other algorithms.

5. Summary and Future Work

In this paper, we offer a new picture encryption system that leverages an elliptic curve key-based ElGamal encryption arrangement for efficient data hiding in images and can be reversed during decryption. In addition, it employs the difference technique already developed for hiding information in photos. Experiments performed in this paper demonstrate that the proposed method is superior to similar schemes in terms of security and computation complexity. An additional step in the right way could be the implementation of a novel data hiding strategy with the aid of smart agents. Experiments have been carried out for the evaluation of the suggested model, and superior performance has been achieved in terms of quick transmission, increased security, no loss compression/decision making on medical image transmission. As a possible next step, researchers are considering

eISSN 1303-5150

implementing a new picture compression method to speed up the transfer of medical images. An additional step in the right direction could be the implementation of a novel data hiding strategy with the aid of smart agents. Applying different rules to new conditions is when intelligent agents really shine. Based on the results of the study of the real facts and the standard rules, developers can create the intelligent rules. The introduction of fuzzy logic during rule formulation allows for the incorporation of intelligence.

6. Reference

[1] Soni P, Pal AK, Islam SH. An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Computer methods and programs in biomedicine. 2019 Dec 1;182:105054.

[2] Haque SA, Aziz SM, Rahman M. Review of cyber-physical system in healthcare. international journal of distributed sensor networks. 2014 Apr 27;10(4):217415.

[3] Raja Krishnamoorthy, T.Jayasankar, S.Shanthi,M.Kavitha,C.Bharatiraja, "Design and implementation of power efficient image compressor for WSN systems," Materials Today: Proceedings, vol.45, part 2, 2021,pp.1934-1938,

[4] Shanthini B, Swamynathan S. Genetic-based biometric security system for wireless sensor-based health care systems. In2012 International Conference on Recent Advances in Computing and Software Systems 2012 Apr 25 (pp. 180-184). IEEE.

[5] Mahapatra B, Krishnamurthi R, Nayyar A. Healthcare models and algorithms for privacy and security in healthcare records. Security and privacy of electronic healthcare records: Concepts, paradigms and solutions. 2019 Dec 13:183.

[6] KiranmaiBellam, N. Krishnaraj, T. Jayasankar, N. B. Prakash, and G. R. Hemalakshmi, "Adaptive Multimodal Image Fusion with a Deep Pyramidal Residual Learning Network," Journal of Medical Imaging and Health Informatics (2020), Volume 11, Number 8, August 2021, pp. 2135-2143,ISSN: 2156-7018 (Print): EISSN: 2156-7026 (Online), IF.0.549

[7] Gardašević G, Katzis K, Bajić D, Berbakov L. Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare. Sensors. 2020 Jun 27;20(13):3619.

[8] K. Muthumayil, R. Karuppathal, T. Jayasankar, B. Aruna Devi, N. B. Prakash, and S. Sudhakar, "A Big Data Analytical Approach for Prediction of Cancer Using Modified K-Nearest Neighbour Algorithm," Journal of Medical Imaging and Health Informatics (2020), Volume 11, Number 8, August 2021, pp.

2184-2189, ISSN: 2156-7018 (Print): EISSN: 2156-7026 (Online), IF.0.549

[9] Xiaotian, W. and Ching-Nung, Y. (2019), 'Partial reversible AMBTC-based secret image sharing with steganography', Digital Signal Processing 93, 22–33.

[10] Wei, W., Chunqiu, W. and Min, Z. (2014), 'Resource optimized TTSH-URA for multimedia stream authentication in swallowable-capsule-based wireless body sensor networks', IEEE Journal of Biomedical and Health Informatics 18(2), 404–410.

[11] Alexey G, F. and Anton A, F. (2017), 'Information attacks and security in wireless sensor networks of industrial SCADA systems', Journal of Industrial Information Integration 5, 6–16.

[12] Zhili, C., Liusheng, H., Haibo, Miao amd Wei, Y. and Peng, M. (2011), 'Steganalysis against substitution-based linguistic steganography based on context clusters', Computers and Electrical Engineering 37(6), 1071–1081.

[13] Amir Hossein, G. and Jalil Seifali, H. (2018), 'A network steganographic approach to overlay cognitive radio systems utilizing systematic coding', Physical Communication 27, 63–73.

[14] Javaid A, K., Nazir A, L., Shabir A, P., Muhammad, K., Javaid, A. S. and Bhat, G.(2019), 'A reversible and secure patient information hiding system for iot driven e-health', International Journal of Information Management 45, 262–275.

[15] ao, Q. (2014), 'A fast algorithm for matrix embedding steganography', Digital Signal Processing 25(25), 248–254.

[16] Wei, W., Chunqiu, W. and Min, Z. (2014), 'Resource optimized TTSH-URA for multimedia stream authentication in swallowable-capsule-based wireless body sensor networks', IEEE Journal of Biomedical and Health Informatics 18(2), 404–410.

[17] Guanglou, Z., Rajan, S., Wencheng, Y., Craig, V., Li, Q., Mehmet A, O. and Subhas Chandra, M. (2019), 'A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices', IEEE Sensors Journal 19(3), 1186–1198.

[18] Liu, G., Liu, B., Liu, X., Li, F. and Guo, W. (2015), 'Low-complexity secure net- work coding against wiretapping using intra/inter-generation coding', China Communications 12(6), 116–125.

[19] Qin, Y, Wang, H, Wang, Z, Gong, Q & Wang, D 2016, 'Encryption of QR code and grayscale image in interference-based scheme with

high quality retrieval and silhouette problem removal', Optics and Lasers in Engineering, vol. 84, pp. 62-73.

[20] Seyedzadeh, SM &Mirzakuchaki, S 2012, 'A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map', Signal Processing, vol. 92, no. 5, pp. 1202-1215.

[21] Seyedzadeh, SM, Norouzi, B, Mosavi, MR &Mirzakuchaki, S 2015,'A novel color image encryption algorithm based on spatialpermutation and quantum chaotic map', Nonlinear Dynamics, vol. 81,pp. 511-529.

[22] ang, Z, Song, J, Zhang, X & Sun, R 2016, 'Multiple-image encryption with bit-plane decomposition and chaotic maps', Optics and Lasers in Engineering, vol. 80, pp. 1-11.

eISSN 1303-5150