SECURE MEDICAL IMAGE ENCRYPTION FOR REMOTE VIRTUAL DOCTOR SYSTEM BASED ON H-IOT APPLICATIONS OVER 5G NETWORK: A COMPARISON STUDY

[1] Fatima Rougaii, [2] Tomader Mazri

[1] Department of Electrical Engineering and Telecommunication Systems, National School of applied sciences, Laboratoryengineering of advanced systems, fatima.rougaii@gmail.com
[2] Department of Electrical Engineering and Telecommunication Systems, National School of applied sciences, Laboratoryengineering of advanced systems, tomader.mazri@uit.ac.ma

KEY WORDS: Remote virtual doctor system (RVDS), Encryption methods, Healthcare IOT applications(H-IOT), Fifth generation network (5G), Medical image.

ABSTRACT:

Recent years have seen a new amalgamation between Remote virtual doctor systems and healthcare IoT applications which plays a crucial role in enhancing patient's healthcare life. The Remote VDS connected with smart Healthcare devices through the wireless network to be accessible anytime and anywhere is anticipated to treat rapidly valuable and confidential data such as personal medical images. Therefore, quick medical image encryption is an essential task in healthcare topic. Some medical image encryption research like the Scan methodology proposed for Remote VDS suffers from a long computational time. Then, the patient will confront difficulty on treatment availability in real-time and especially for critical situations. To overcome this problem, in this work, three medical image encryption methods are compared, (1) A Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications, (2) A new chaotic map with dynamic analysis and encryption application on the Internet of Health Things, and (3) Robust medical image encryption based on DNA chaos method. The comparison results have proven that the new chaotic map with a dynamic analysis scheme has high-security analysis and performances with low computational time compared to other methods. That makes it a good candidate for the H-IOT-RVDS environment connecting over 5G technology like a cellular network to enable connectivity between nodes.

1. INTRODUCTION

Medical innovations nowadays are becoming an increasingly important lever inquest of improving efficiency. Some patients and especially those who live in rural areas far from hospitals could be treated rapidly without minimizing the healthcare quality due to telemedicine services such as video conferencing or other virtual technologies (Abid et al, 2021). In addition, providing a real-time monitoring of individual's health conditions, quick access to the database, Rapid diagnosis, prevention in critical situations, and first detection of improvements in related health patterns of the patient (Mallios, 2018). These qualities are offered by the combination of both developed technologies; the Virtual Doctor (VD) system and healthcare IoT applications. Therefore, they can present a real-time reaction to individuals with critical health conditions and continuously monitor the health status of the patient by integrating the medical wearable devices (Mallios, 2018);

The virtual doctor system provides continuous monitoring of the patient's health, Also, it connects with the patients by performing a dialogue with them, and realize a reliable diagnosis that is checked by a professional. Furthermore, in emergency situations the VDS capable to provide the first intervention and identify changes in health patterns (Mallios et al, 2015). On the other hand, Virtual doctors can also obtain various medical specialties. For example, virtual dental, virtual ortho, virtual coach, virtual emergency, virtual cardio, virtual Gynecologist (Furht et al, 2013) …. In some cases, the VDS has to diagnose the patient in the hospital and then requires its presence in this Place (Fujita et al, 2010 ; Naim et al, 2019 ; Fujita et al, 2010). However, in other cases, the VD machines can remotely treatthe patient with the help of smart health care technology (Karthik et al, 2014; Barakah et al, 2012; Venkataraman et al, 2020).

The RVD process demands and uses medical imaging tests to make the disease diagnosis and provides accurate treatment for the patient. So, some type of medical images should be captured by medical smart devices or other specific medical systems and shared with RVDS in order to treat health condition of patient. According to the previous RVDSs, the artificial medical diagnostic system (Karthik et al, 2014) is accurately based on tongue images analysis. Also, the Virtual heart doctor (Venkataramanaiah et al, 2020). determines its diagnosis based on ECG signal. Some others requested medical imaging tests such as MRI, X-Rays … can be used to determine diagnosis diseases. Generally, the sensitive medical images shared between H-IOT and RVDS shouldn't be divulged to the public to ensure patient's privacy, so just legitimate parties (doctor and patient) have access to this information.

Throughout the study on RVDS security topics, it is remarked that there's a lack of medical image encryption mechanisms and the only presented design is proposed by Mallios et al (Mallios et al, 2014). The scheme is called Compression-Hiding-Encryption and performed on the patient node. The authors Utilize this scheme in wearable health monitoring systems for biosignals transmission. It is based on the SCAN method and presents lossless compression, strong information hiding, and robust encryption. Scan pattern technique is characterized by lossless compression encryption (good ratio), Robust information hiding (hide 12,5% of the original image) (Maniccam et al, 2004), and had a high level of security compared to base switching and entropy coding image compression-encryption methods (Yang et al, 2004).

Nevertheless, this method requires a long Compression-encryption time (Maniccam et al, 1999). It can take 7 seconds as an encryption-compression time for a medical image of size 256×256. And 54 seconds for Lena 512×512 (Maniccam et al, 2001). Furthermore, the video of 20 frames can require 5 second as Compression- encryption and decompression-decryption (s) (Bourbakis et al, 2003)

So, the main contribution of this work is to find a fast and robust medical images encryption method to ensure the confidentiality and privacy of the patient. Also treat rapidly the patient conditions status and especially in critical situations. In this study, some medical image encryption methods used in smart healthcare applications are exploited. The chosen encryption methods have to treat the same medical image characteristics considering the type and the size of image in order to get an exact comparison and accurate results. Therefore, Hassan et al, 2021) introduce a Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications to protect the confidentiality of patient's medical images. A new chaotic map with dynamic analysis andencryption application on the Internet of Health Things is proposed by (Tsafack et al, 2020) for securing the transmission of the medical images in the H-IoT environment. Finally, (El- Shafai et al, 2021) develop Robust medical image encryption based on DNA chaos method as a strong cryptosystem for securing telemedicine and healthcare application.

Smart healthcare technology can transfer medical images to RVDS via 5G network as a suggested cellular network that delivers fast and reliable data sharing. Moreover, this network presents 100 megabits per second as speed, more data bandwidth, support 50 billion connected devices, and 212 billion connected sensors (Li et al, 2018). These previous characteristics can incorporate a connected and fully involved environment with many applications; artificial intelligence, enhanced mobile broadband, machine-to-machine communications, and advanced digital services (West et al, 2016). On the other hand, the Virtual Doctor System utilizes medical wearable sensors to evaluate a patient's signs and serve the patient to obtain a particular diagnosis. So, due to the fifth-generation network connection, the virtual health world can diagnose and control a patient in real-time. The medical data will be shared remotely and reliably in a few seconds, and the patient will be informed about his status immediately and continuously. Finally, the combination of Remote VDS, H-IoT applications, and 5G technologies will reveal a new healthcare world challenge.

The remaining part of this paper is organized as follows: the related medical images encryption schemes for H-IoT applications are described in section 2. A comparison study is presented in section 3. Section 4 discusses the comparison results. Section 5 shows a secure medical image transmission for remote VDS architecture based on H-IoT applications over a 5G network. Section 6 concluded the paper.

2. RELATED WORKS

2.1 Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications

(Hassan et al, 2021) introduced an efficient and lightweight encryption scheme to protect the privacy of the patients' medical image for the healthcare industry. The algorithm uses two permutation methods to achieve secure medical image encryption. It is formed in a three-stage process. In the first stage, the output of the transition operation is transferred as an input, and the first step's output is transferred as an input to stage two. Ultimately, passing the second stage's output as an input to the third stage. Throughout the entire process, the shuffling operation with 256-bit key-value utilizing logical operation is applied.

Generally, the procedure of this technique is maintained as follows:

1. Configuring the parameters.
2. Applying the key for the images.
3. Staring the Key nomination and Image nomination process.
4. Doing the compute and applying the block-based Image encryption transformation and the proposed lightweight Image encryption scheme.
5. And Check for the calculation of the best data (Hassan et al, 2021).

The authors used an experimental approach to determine the scheme's performance. They are considered four images for the test where the image's size is 512 x 512 pixels with 8 bits per pixel (bpp) in the grayscale image. The encryption method was analyzed, evaluated, and compared to other conventional encrypted techniques in terms of performance and security analysis. Therefore, the medical image encryption mechanism has a higher performance analysis concerning encryption speed that equals 0,1 MB/s, a good encrypted entropy near to the ideal value 8. Also achieving better efficiency by having lower encryption/decryption time, higher peak signal-to-noise ratio (PSNR), and superior mean-square error (MSE) compared to other methods.

2.2 A new chaotic map with dynamic analysis and encryption application in Internet of Health Things

(Tsafack et al, 2020) proposed a new chaotic map with dynamic analysis, this effective cryptosystem aims to secure the medical images communication in an Internet of Healthcare Things (IoHT) environment. Generally, the scheme's process begins by creating a 2-D trigonometric that utilize Some of the most famous dynamic analysis mechanisms, namely the Bifurcation diagram, Lyapunov exponent, and phase space trajectories to clarify the map's chaotic dynamic. Next, the authors employ four elements: Mandelbrot set, new conditional shift function, Bit-XOR function, and the constructed trigonometric map to design a new medical color image encryption.

In detail, the algorithm is designed as follow; firstly, split a received image from healthcare devices into three components R, G, B. Then generate three sets of key streams from the newly formed trigonometric map as well as utilize these keys jointly with the parts of image (R, G, B) for computing the hamming distance. After that, the Bit-XORed operation is implemented between the output distance vector corresponding to each part of image and every key stream, and save the output and use it for further processing. Moreover, the keys streams and the decomposed components are Bit-XORed again to generate an output, this output is fed into the algorithm of conditional shift. Use the Mandelbrot set as an input to the algorithm of conditional shift. then apply the confusion function (complete shuffling of pixels) in the algorithm. As a final step, the Bit-XORed (Diffusion) is performed between the resultant shuffled vectors and saved outputs, and then combine the image vectorsto generate the encrypted image.

Moreover, the algorithm used several metrics for experimental tests validation. So, the experiments' results indicate that the trigonometric encryption scheme has a minimal value of correlation coefficient in vertical, horizontal, and diagonal directions. It reaches high randomness in the encrypted images due to the high encrypted entropy value close to 8. Besides, it gets a high number of pixels to change rate (NPCR) and unified averaged changed intensity (UACI) which proves that the encryption algorithm is unbreakable. Furthermore, the histogramof encoded images analysis presents uniformity in the pixels' distribution that demonstrates the robustness of the cryptosystemagainst attacks. The key space study shows that the encryption scheme provides a large key space greater than 2^{100}. Finally, the analysis part indicates that the scheme has a high security level due to resistance against various attacks, such as noise attack, occlusion attack, statistical attack, differential attack, brute-force attacks, known-plaintext attack, and chosen-plaintext attack. And gets good performances analysis that proves its suitability for the Internet of Healthcare Things environment to secure medical images transmission.

2.3 A Robust medical image encryption based on DNA chaos cryptosystem for secure telemedicine and healthcare application

(El-Shafai et al, 2014) created a robust and efficient medical image encryption technique for smart healthcare devices. The authors' contribution aims to combine the chaos techniques and the advantage of de-oxyribo nucleic acid (DNA) in a single encryption process to highly secure the medical images communication utilized in healthcare services and telemedicine. Moreover, other tools such as Piecewise linear chaotic map (PWLCM), DNA encoding, and Logistic chaos map exploited together to get the encryption parameters needed to design ciphered medical images. At first, the PWLCM technique generates a secret key image. And The DNA rules are employed for encoding the input plain image and secret key image. After that, the logistic map is utilized to create an intermediate image as another secret key image to install the functions of DNA row-by-row on the coded original image. Furthermore, the intermediate image is decoded in the following step. At last, the precedent processes are iterated over image columns once again to realize the ideal encrypted image.

The experimental tests are realized on the medical image size of 256×256 considering 8-bits per pixel. This medical image cryptosystem can encipher grayscale/color and medical/non-medical images types. In addition, the scheme is evaluated and tested through some metrics-based pixels properties, diffusion quality, and Miscellaneous. Experimental results and comparisons indicate that the encryption method provides good entropy encryption close to the optimum value of 8. also has Low correlation coefficient values. Besides, high UACI and NPCR values are close to the optimum values, good structural similarity (SSIM) index, and good feature similarity (FSIM). In addition, it has a low value of Peak Signal-to-Noise Ratio (PSNR) for the ciphered image implies the efficiency of the medical image cryptosystem compared to other methods. Also, it offers good key sensitivity for slight changes in the secret key, large key space, and low running time. Finally, the histogram uniformity evaluation demonstrates the performance efficiency of the encryption/decryption process.

Therefore, the scheme achieves superior performances analysis for medical image transmission and has higher robustness and security. Thus, it can fight various known attacks, such as known-plaintext and chosen-plaintext attacks, differential attacks, statistical attacks, and noise attacks.

3. COMPARATIVE ANALYSIS

3.1 Principal metrics

In this section, the three medical image encryption methods employed for smart healthcare applications are compared. A detailed comparison study is provided in terms of their performance analysis (correlation, NPCR, UACI, SSIM, PNSR, and entropy) to prove the robustness and efficiency of the cryptosystem. The computational time analysis demonstrates the quickness of the protocol, and finally the security analysis.

3.1.1 Correlation: The independence property can be evaluated by testing the correlation between original and ciphered images in three directions (horizontal, vertical, and diagonal). The statistical parameter value ought to be almost closer to zero (Noura et al, 2019). It is recommended to get a lower correlation value of the encrypted image compared to that of the original image to reach a high ciphering performance against statistical attacks.

3.1.2 NPCR (number of pixels change rate): The number of pixels change rates (NPCR) is measured to assess the impact of a minor change of the original image on its encrypted image (Khashan et al, 2020). The NPCR parameter is used to determine the ratio of distinct pixels between two encrypted medical images. It is necessary to get optimum NPCR value which ought to be large enough and more than 99% to avoid differential attacks (El-Shafai et al, 2014).

3.1.3 UACI (unified averaged changed intensity): The UACI indicates the quantity of average intensity of dissimilarities amongst two encrypted medical images such as NPCR. The optimum value of UACI implies better encryption (El-Shafai et al, 2014). The UACI value needs to be large enough and greater than 33% To resist differential attack.

3.1.4 SSIM (structural index similarity): When the SSIM value is closer to 1, this indicates a high similarity between compared images. Otherwise, if a value of SSIM is closer to 0, this means they are completely different (Khashan et al, 2020).

3.1.5 PNSR (peak signal to noise ratio): In the presence of Chanel noise, The PNSR is utilized to determine the robustness of the medical image encryption scheme. It is estimated between the plain and encrypted medical images. Ciphered images must get a low PNSR value. And high PNSR values for deciphered images (El-Shafai et al, 2014). Generally, when PNSR is larger than 34 DB, it indicates that the quality of the image is acceptable. And both images are typically indistinguishable by a human if PNSR is higher than or equal to 40db (Khashan et al, 2020).

3.1.6 Entropy: Entropy metric refers to the quantity of data hidden in an image. It evaluates the degree of randomness in the encryption system (Tsafack et al, 2020). Furthermore, a random image should take the value 8 as an optimal value for the entropy. Then, reaching a better encrypting process and the chance of predictability will be minimized (Parameshachari etal, 2020).

3.2 Performance analysis comparison

Several metrics can be evaluated from Table 1. Firstly, the correlation parameter is measured in each of the methods 2

and From the presented values, the method 2 reaches a minimal correlation value in the three directions, which is better than the method 3. In addition, a good cryptosystem should obtain an NPCR close to 100% and 33% as a good value of the UACI metric. So, the UACI of the method 2 is slightly higher than the method 3. Generally, both schemes get an NPCR greater than 99,60 %, and the comparison of metrics values presents that the NPCR of the scheme 3 is higher than the other scheme 2. Moreover, the PSNR's comparison of existing schemes demonstrates that the PSNR of the method 3 is much larger than method 1, which indicates that the first method 1 gets an effective PSNR. Furthermore, the SSIM is measured just in the scheme 3 and is very close to 0. At last, the entropy metrics are assessed on the three methods, and it is noticed that the methods 2 and 3 get 7,99 as entropy values which are higher than method1.

Metrics	Method 1 (Hassan et al, 2021)	Method 2 (Tsafack et al, 2020)		Method 3 (El-Shafai et al, 2014)	
Correlation Of encrypted data	---	H	0,00267	H (Average)	0,0136
		V	-0,00008	V (Average)	0,0097
		D	-0,00007	D (Average)	-0,0033
NPCR (%)	---	99,63		99,69	
UACI (%)	---	33,53		32,24	
SSIM (DB) (Average)	---	---		0,0039	
PSNR (DB)	39	---		52,73	
Entropy	7,98	7,99		7,99	

Table 1: The comparison of metric's evaluation

3.3 Comparison of running time analysis

Running time presents one of the crucial measures used to evaluate the performance of an algorithm. An encryption scheme should take less computational time to be used successfully in encrypting images.

Table 2 compares the running time's evaluation measures of encryption schemes on 256*256 resolution and 512*512 resolution images. As seen from Table 2, method 2 takes 0,65 seconds for each 512*512 resolution image which is much lower than method 1. Also, for the image of size 256*256, it is observed that the running time of scheme 2 is significantly less compared to scheme 3, which is much greater than 3 seconds.

Image size	Running time (second)		
	Method 1 (Hassan et al, 2021)	Method 2 (Tsafack etal, 2020)	Method 3 (El-Shafai et al, 2014)
512*512	2,75 (Average)	0,65	---
256*256	---	0,26	3,12 (Average)

Table 2: Running time comparison of existing methods

3.4 Security analysis comparison

Attacks		Resistance of attacks		
		Method 1 (Hassan et al, 2021)	Method 2 (Tsafack et al, 2020)	Method 3 (El-Shafai Et al, 2014)
Key Security analysis	Key space attacks	---	Yes	Yes
	Key sensitivity attacks	---	---	Yes
	Key randomness attacks	---	---	---
Ciphertext onlyattacks		---	---	
Known plaintextattacks		---	Yes	Yes
Chosen plaintextattacks		---	Yes	Yes
Chosen ciphertext attacks		---	---	---
Differential attacks		---	Yes	Yes
Statistical attacks:		Yes	Yes	Yes
Noise attacks		---	Yes	Yes
Occlusion attacks		---	Yes	---

Table 3: security analysis's comparison of existing methods

Table 3 shows the comparison of security analysis between methods. So, it is observed that both methods 2 and 3 are commonly free from key space attacks, known- plaintext attacks, chosen-plaintext attacks, differential attacks, Statistical attacks, and noise attacks. In addition, only method 2 can withstand occlusion attacks. Finally, the security analysis of method 1 doesn't evaluate before authors, and it can just resist statistical attacks due to its decreased correlation parameter.

3. DISCUSSION PART

This section discusses the comparison's results reached before. As mentioned previously, the absence of medical image encryption used in RVDS enabled H-IoT over 5G exposes a new challenge in this term. And the only suggested encryption method offers high security but is still inefficient in terms of running time. Therefore, the needed medical encryption algorithm should require a high level of security analysis to be strong against various attacks. Besides, having high robustness and efficiency in terms of encryption entropy, PNSR, SSIM, correlation coefficient. Finally, the scheme should have high performances specifically low running time. So, the medical information will be shared in a short time, which makes the medical encryption method more convenient especially in critical situations.

From the previous comparison, it is clear that some medical image schemes used for H-IOT can attain the demanded requirements and others aren't. So, it's evident that the weakest one among the methods is the method (Hassan et al, 2021).

Because even it verifies a low value of PNSR, good entropy, and resist just statistical attacks, but still take a long-running time which makes it not recommended for emergency and critical situations in a RVDS-H-IOT-5G environment.

On the other hand, the two rest methods (Tsafack et al, 2020; El- Shafai et al, 2014) have a high-performance analysis concerning correlation, entropy, NPCR, UACI. In addition, there are differences between both schemes. The method (Tsafack et al, 2020) is still more correlated, has a good UACI and entropy. Moreover, the method (El- Shafai et al, 2014) has many strengths like resisting some kind of attacks, but it still takes a long time of encryption operation that represents a very important requirement to get a fast response from RVDS to patient. However, the method (Tsafack et al, 2020) takes a much lower and best running time, which represents an advancement for this method and helps the patient to receive its diagnosis and treatment quickly from the RVDS. Don't forget that the scheme has a high level of security due to its withstanding of various attacks and specifically occlusion attacks.

As a result, the suitable scheme that represents a crucial choice for the RVDS-H-IOT-5G scenario is the new chaotic map with dynamic analysis and encryption application on the Internet of Health Things (Tsafack et al, 2020). For being very good in terms of security and performance analysis. Besides providing fast process with an effective running time. As a perspective, thealgorithm can be modified in order to encrypt another type of data such as medical video, audio, text in smart healthcare applications.

4. SECURE MEDICAL IMAGE TRANSMISION FOR REMOTE VDS ARCHITECTURE BASED ON SMART HEALTHCARE APPLICATIOS OVER 5G NETWORK

Recently, the healthcare revolution is encouraged by various developments of new technologies. 4G and other network technologies are applied in the healthcare domain for H-IOT applications and services. These communications standards play a significant role in smart healthcare evolution in the future. With the rapid growth in the healthcare field, Various applications are anticipated to produce a large amount of data in several sizes and formats. Such enormous and various data demands particular treatment regarding the end-to-end delay, latency, bandwidth, and other parameters. So, these current technologies are not able to satisfy the requirements of smart healthcare applications. For that reason, a new technology network is developed to cope with various communications needs of H-IOT applications, namely the fifth generation.

In addition, the Fifth generation assisted Healthcare IOT networks are a fusion of IOT nodes that demand some requirements such as ameliorated network performance and reinforced cellular coverage (Ahad et al, 2020). Fifth-generation technology provides several benefits such as high network speed of 10Gbps, ultra-low latency (about 1ms round trip time), super bandwidth in unit area, massive number of connected devices, 99.999% of a perceived availability, 100% coverage, 90% Reduction in energy, High battery life. Related to these previous requirements, different aspects of 5G wireless systems will begin introduced by academia and research organizations (Agiwal et al, 2016). Therefore, 5g enables diverse healthcare applications and systems. For example; artificial intelligence (AI)–powered robotic surgeries, Virtual patient consultation, virtual reality (VR)… (Dananjayan et al, 2021).

In this work, the suggested 5g network provides benefits for smart healthcare applications and RVD systems. Such amalgamation gives an advantage concerning virtual self-diagnosis programs. Moreover, it offers a reduction of hospitalization time, enhancing the health life of the patient by providing a reliable and quick diagnosis. As well as the fast response from RVDS that assist a real doctor for giving final decision besides taking a proper precaution at a convenient time like avoid from diseases complication and gain a rapid surgical intervention in case of need. Such a cellular network can be able to enable efficient communication connectivity between patients and RVDS. So, the medical images captured by a real doctor or medical sensors are transferred to RVDS to offer a diagnosis via a 5G network

.

This part presents an architecture of medical image security in RVDS based on smart healthcare applications connected over a 5g network is presented. Accordingly, the architecture process is shown in figure 1 and includes the following steps: firstly, the sensors capture specific medical images needed for diagnosis. Next, the chosen medical images encryption scheme (new chaotic map with dynamic analysis and encryption application on Internet of Health Things) (Tsafack et al, 2020) is selected and used to encrypt proper medical images.

After the encryption phase, the encrypted medical images are transferred to mobile via Bluetooth connection. The mobile transmits these encrypted images to RVDS using a 5G network. After that, the RVDS receives the enciphered images and decrypts them using the same suggested medical image encryption (new chaotic map with dynamic analysis and encryption application on Internet of Health Things) (Tsafack et al, 2020). Then, the system makes an accurate diagnosis of medical images, and the produced results will be checked by a real doctor to provide a final decision of the patient's health condition. Eventually, the final decision will be transferred from RVDS to the patient to offer the specific treatment to a patient, and when it comes to dangerous situations the server helps the patient by calling an ambulance. After, the VDS transmits these encrypted medical images to the database that is responsible for storing all sensitive medical images to be utilized by physicians as a reference.

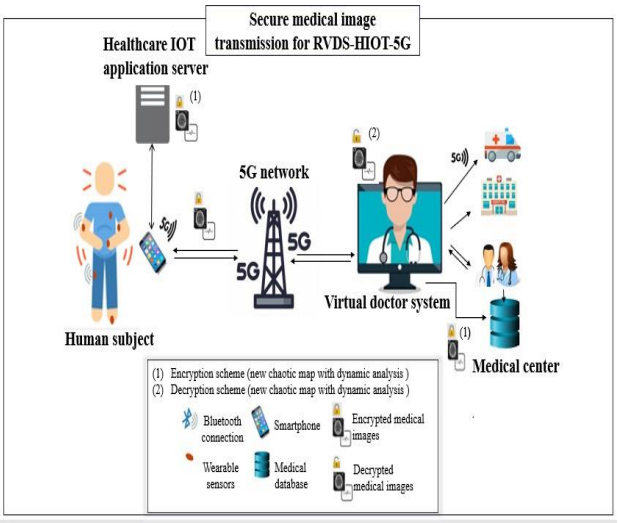

Figure 1. Secure medical image transmission for RVDS- HIOT-5G architecture.

5. CONCLUSION

This paper has compared three medical image encryption schemes for smart healthcare applications. The comparison results show that the new chaotic map with dynamic analysis and encryption application on the Internet of Health Things is chosen as a robust and quick encryption scheme to encrypt medical images for RVDS enabled health-IOT applications through a 5G network.

The comparison study given in this paper can bring helpful insight in creating cryptographic mechanisms for the problem of medical image's encryption search for RVDS enabled smart healthcare applications connected via 5G network with robust security and efficiency requirements. For future work, the comparison results will be validated by a simulation in RVDS-H-IOT-5G scenario.

ACKNOWLEDGEMENTS

The authors sincerely thank the Engineering of Advanced Systems Laboratory for the support.

REFERENCES

Abid, H., Mohd, J., Ravi Pratap, S., Rajiv, S., 2021. Telemedicine for healthcare: Capabilities, features, barriers, and applications. *Sensors International*.

Mallios, S., 2018. Virtual doctor: an intelligent human-computer dialogue system for quick response to people in need.

Mallios, S., Bourbakis, N., 2015. A dialogue monitoring scheme for a virtual doctor. *National Aerospace and Electronics Conference (NAECON)*, 249-253.

Furht, B., Ankur, A., 2013: *Handbook of medical and healthcaretechnologies*. Springer. New York.

Fujita, H., Hakura, J., Korematsu, M., 2010. Virtual doctor system (VDS): Medical decision reasoning based on physical and mental ontologies. *In International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, 419-428. Springer, Berlin, Heidelberg.

Naim, A., Mohammad, F, K., Mohammad, R, H., Nawsher, K., 2019. "Virtual Doctor" Management Technique in the Diagnosis of ENT Diseases. *International Journal of Online and Biomedical Engineering (iJOE)*, 134-140.

Fujita, H., Jun, H., Masak, K., 2010. VIRTUAL MEDICAL DOCTOR SYSTEMS-Status Progress Report on Virtual Medical Doctor System (VDS) Interaction Interface. *International Conference on Health Informatics*, 38-45.

Karthik, R., Menaka, R., Kulkarni, S., Deshpande, R., 2014. Virtual doctor: an artificial medical diagnostic system based on hard and soft inputs. *International Journal of Biomedical Engineering and Technology*, 329-342.

Barakah, D, M., and Muhammad, A., 2012. A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. *Third International Conference on Intelligent Systems Modelling and Simulation*. *IEEE*, 214- 219.

Venkataramanaiah, B., Kamala, J., 2020. ECG signal processing and KNN classifier-based abnormality detection by VH-doctor for remote cardiac healthcare monitoring. *Soft Computing*, 17457-17466.

Mallios, S., and Nikolaos, B., 2014. A virtual doctor prototype for quick diagnosis and secure health information exchange. *The 5th International Conference on Information, Intelligence, Systems and Applications. IEEE*, 260-265.

Maniccam, S, S., Bourbakis, N, G., 2004. "Lossless compression and information hiding in images,". *Pattern Recognition*, 475–486.

Yang, M., Bourbakis, N., Shujun, Li., 2004. Data-image- video encryption. 23(3), 28–34.

Maniccam, S, S., Bourbakis, N; G., 1999. "SCAN based lossless image compression and encryption,". *in Proceedings 1999 International Conference on Information Intelligence and Systems*, 490– 499.

Maniccam, S, S., Bourbakis, N, G., 2001. "Lossless image compression and encryption using SCAN,". *Pattern Recognition*, (34)6, 1229– 1245.

Bourbakis, N, G., Dollas, A., 2003. "SCAN-based compression-encryption hiding for video on demand,". *Multimed, IEEE*, (10)3, 79–87.

Hasan, M, K., Islam, S., Sulaiman, R., Khan, S., Hashim, A, H, A., Habib, S., Alyahya, S., Kamil, S., Hassan, A, M, A., 2021. Lightweight encryption technique to enhance medical image security on internet of medical things applications. *IEEE Access*, 9, 47731-47742.

Tsafack, N., Sankar, S., Abd-El-Atty, B., Kengne, J., Jithin, K, C., Belazi, A., Abd El-Latif, A 0, 2020. A new chaotic map with dynamic analysis and encryption application in internet of healththings. *IEEE Access*, 8, 137731-137744.

El-Shafai, W., Khallaf, F., El-Rabaie, E, S, M., Abd El-Samie, F, E., 2021. Robust medical image encryption based on DNA- chaos cryptosystem for secure telemedicine and healthcare applications. *Journal of Ambient Intelligence and Humanized Computing*, 1-29.

Li, S., Da Xu, L., Zhao, S., 2018. 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, 10, 1-9.

West, D, M., 2016. How 5G technology enables the health internet of things. *Brookings Center for Technology Innovation*, 3, 1-20.

Noura, H., Chehab, A., Noura, M., Couturier, R., Mansour, M M., 2019. Lightweight, dynamic and efficient image encryption scheme. *Multimedia Tools and Applications*, 78(12), 16527-16561.

Khashan, O, A., AlShaikh, M., 2020. Edge-based lightweight selective encryption scheme for digital medical images. *Multimedia Tools and Applications*, 79(35), 26369- 26388.

Parameshachari, B, D., Panduranga, H, T., liberata Ullo, S., 2020. Analysis and computation of encryption technique to enhance security of medical images, 925(1), 012028.

Ahad, A., Tahir, M., Aman Sheikh, M., Ahmed, K I., Mughees, A., Numani, A., 2020. Technologies trend towards 5G network for smart health-care using IoT: A review. *Sensors*, 20(14), 4047.

Agiwal, M., Roy, A., Saxena, N., 2016. Next generation 5G Wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 18(3), 1617-1655.

Dananjayan, S., Raj, G, M., 2021. 5G in healthcare: how fast will be the transformation? *Irish Journal of Medical Science*, 190(2), 497-501.