Egyptian Journal of Medical
Human Genetics

RESEARCH

Open Access

# Secure framework for IoT technology based on RSA and DNA cryptography

Mona M. Elamir[1*], May S. Mabrouk[2] and Samir Y. marzouk[3]

## Abstract

**Background:** The Internet of things (IoT) is the network of different objects or "things" containing sensors, software, and other technologies used to exchange data between devices and systems over the cloud. Such systems and networks should be provided with a proper cryptographic methodology to block unauthorized data transmission access. This issue is considered an essential challenge of resources that are shared on the data communication network, that is its security. So, in this study, a cryptosystem is proposed to maintain the security level of such systems with a new idea depending on DNA cryptography and DNA mixing.

**Results:** In this study, the proposed cryptosystem is based on the RSA algorithm and DNA cryptography concepts with a novel idea for mixing DNA strands obtained from encoding medical image and report to enhance the security level through the IoT networks. This system achieved a proper result in reconstructing images with high quality. The similarity between the original data and the restored one reached 92% through 18 s.

**Conclusions:** Such a proposed cryptosystem provided the feasibility of data security in network security, especially for E-health care through IoT system to help medical teamwork in handling medical data between hospitals safely. The result showed that RSA is a fast, efficient algorithm that can be utilized safely in cryptography schemes.

**Keywords:** RSA algorithm, Image encryption, DNA cryptography, IoT security

## Introduction

Cryptography plays an important role in data protection in the applications that run through the public network which allows people to achieve their business electronically without worries of deceit, in addition to keeping the security and the integrity of the message and the sender authenticity. So, it has become more essential in our daily life as most people interact electronically every day, through e-mail, e-commerce, ATMs, cellular phones, etc. This increase in data transmitted has made increased the reliance on cryptography algorithms and authentication by users [1]. Although secured communication has existed over centuries, the key generation problem has prevented it from a familiar application. The development of key cryptography has enabled a large-scale network of users that can communicate securely with one another even if they had never communicated before [1].

Cryptography contains the following two main categories according to the key used:

(i) Symmetric key cryptography: Both the sender and the receiver use the same secret key in encryption and decryption like AES, DES, etc.

(ii) Asymmetric key cryptography: It contains two keys, the first one is public and the second one is kept secret; both the keys work in pairs of matched public and private keys like the RSA algorithm [2].

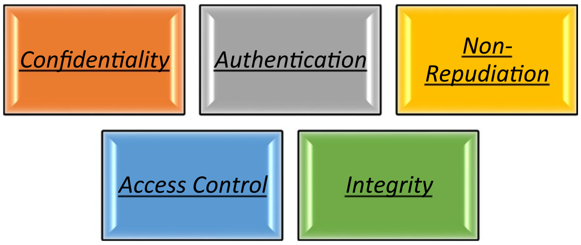
Cryptography provides the required security to ensure data privacy and its non-alteration. The most essential cryptography goals are as follows [1]:

A. *Confidentiality* The transmission of data from one computer to another computer must be accessed by an

*Correspondence: Eng.mona.elamir@gmail.com

[1] Biomedical Engineering Department, Helwan University, Cairo, Egypt
Full list of author information is available at the end of the article

authorized user and it does not be accessed by anyone else.



B. *Authentication* The transmission of data from one computer to another computer must be accessed by an authorized user and it does not be accessed by anyone else.

C. *Integrity* Only the authorized party can modify the transmitted information. And an unauthorized person should not allow modifying the sender and receiver.

D. *Non-Repudiation* Ensures the message that the sender or the receiver should be able to deny the transmission.

E. *Access Control* The authorized persons are only able to access the information while in transfer.

One of the major applications, that require Confidentiality as an essential concept in transmitting data over the cloud, is the Internet of things (IoT). IoT is considered a system of related devices like objects, mechanical machines, animals, or humans which provide the ability to transfer data over a network without requiring human-to-computer interaction [3]. Each IoT system is consisting of a smart device that is Web-enabled to use in the embedded systems, like sensors, processors, and hardware, to either handle or send or act on the acquired data from their environments.

The importance of the Internet of things can be summarized by helping people to work and live smarter and access complete control over their lives. Not only do IoT smart devices offer automated homes, but also they are essential for business as they provide a real-time look into how their systems work, delivering insights into everything from the performance of machines to supply chain and logistics operations. As such, IoT is one of the most important technologies of everyday life, and it will continue to pick up steam as more businesses realize the potential of connected devices to keep them competitive.

## Related works

Many researchers have proposed different studies depending on many algorithms like a study for Reza Fotohi and others who have used the RSA algorithm and interlock protocol to prevent denial-of-sleep (DoS) attacks that threatened the sensor nodes in wireless sensor networks [4]. Min Liu and Guodong Ye have proposed an asymmetric image encryption algorithm based on DNA coding and a hyperchaotic system by generating the initial values of the hyperchaotic system from the RSA (Rivest–Shamir–Adleman) algorithm and then permutation of the image pixels to confuse the image according to the chaotic sequences generated [5]. Also, Al-Obeidi and others have proposed a hybrid synchronization of high-dimensional chaos with self-excited attractors based on a hyperchaotic system [6]. Lin and Li have proposed an image encryption scheme based on Lorenz hyperchaotic system and Rivest–Shamir–Adleman (RSA) algorithm by generating the initial values of the chaotic system from the RSA algorithm; they proved that their experimental results prove that the image encryption scheme proposed in this research is effective and has strong anti-attack and key sensitivity. Moreover, the security of this encryption scheme relies on the RSA algorithm, which has a high security level [7]. Mir et al. have proposed an asymmetric encryption scheme for color images by introducing an efficient triple-layered encryption scheme based on the RSA cryptosystem along with a chaotic map in the discrete Hartley domain. In the proposed system, the image is encrypted using the RSA and then transformed into discrete Hartley domains to diffuse the image pixels; these pixel positions are dislocated by applying a nonlinear chaotic map to provide a complex structure of the scheme [8]. Another study by Nentawe Y. Goshwe has designed a GUI on Java to encrypt messages using the RSA algorithm; his application GUI package contains four categories: MainApp.java, Receiver-Interface.java, Sender-Interface.java, and Table-Display.java. The dB-Interface package only contains the Retrieve-Message.java and the Send-Message.java class. The encoding-and-decoding package contains the Encoding-And-Decoding.java class [9]. Hoyoung Yu and Y. Kim and others have proposed a new RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices. Such key has been generated from a true prime random number generator (TPRNG), which generates a prime number that cannot be predicted [10]. Babo and others have proposed new multi-image encryption using a combination of three algorithms: chaotic permutation techniques (Arnold Cat map), RSA algorithm, and DNA sequence encoding. In their proposed system, each image with size 256*256 has been divided into four blocks which then encrypt each block with a key generated from a chaotic map and then encode blocks into DNA format. They have evaluated their system using entropy, NPCR, UACI, and histogram analysis [11].

## Materials and methods

In this study, a cryptosystem has been designed to encrypt both medical images and medical diagnostic reports to enhance the security of E-health technology in saving sensitive medical data. Through encryption, both medical images and medical reports have been encrypted using an RSA algorithm with a public key (p) and then encode the encrypted image into DNA format using encoding rules with a number equal to (*p* value) (the public key) under condition $p < 8$ (the maximum number of encoding rules); the same in the encrypted medical report has been encoded into DNA using (q) encoding rule (under the same condition). Finally, both DNA strands have been mixed with a ratio equal to (p/q) getting the final encrypted data in DNA format. The encryption process is shown in Fig. 1.

Through decryption, the reverse sequence has been applied to start with separating mixed DNA strands into two strands by dividing the ratio (p/q). These two strands have been decoded each one by the same encoding rule.

(p-rule for image and q-rule for report). Finally, these decoded data have been decrypted using RSA with a private key to restore the original data as shown in Fig. 2.

Dataset:

The dataset used in this study has been acquired from the Kaggle Web site that contains MRI tumor brain images which are divided into 98 normal brain images and 155 abnormal brain images [12].

RSA:

RSA algorithm is one of the common asymmetric key cryptosystems that is widely used for securing data through transmission. In such a cryptosystem, the encryption key is a public one and the decryption key is private and kept secret [13]. The security in the RSA algorithm is based on the product of two large prime numbers. RSA algorithm is based on three major steps as mentioned in Table 1: (1) key generation, (2) encryption, and (3) decryption:

## Key generation

In this step, the RSA algorithm calculates both the public key and private key from the two prime numbers as follows:

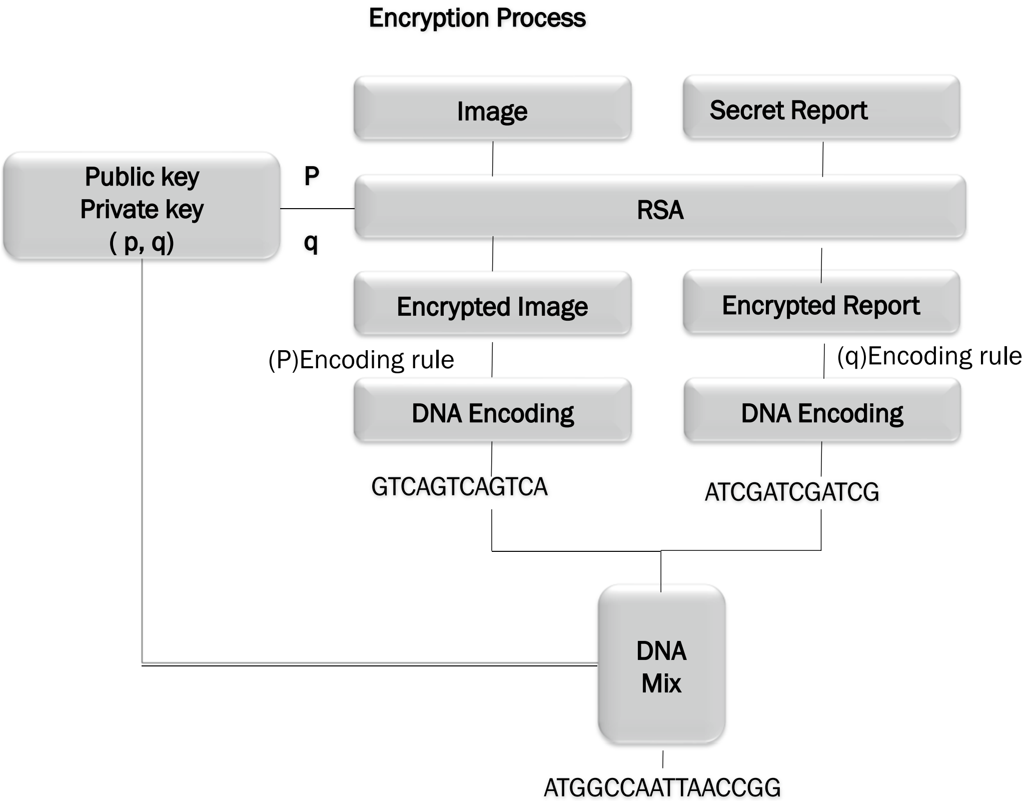


**Fig. 1** Encryption process of the proposed cryptographic system

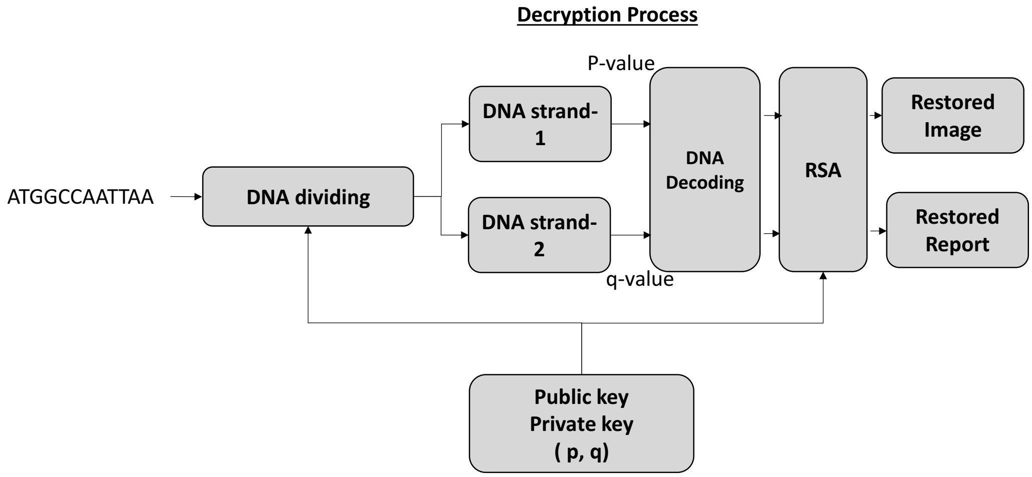


**Fig. 2** Decryption process of the proposed cryptographic system

**Table 1** RSA procedures

| # | Step |
|---|---|
| **1** | Choose two prime numbers p and q (p≠q) |
| **2** | Compute "n value" such $n = p * q$ |
| **3** | Compute φ(n):$\varphi(n) = (p-1)(q-1)$ where φ is Euler's totient function |
| **4** | Choose an integer (e) such that:<br>$1 < e < \varphi(n), \&gcd(e, \varphi(n)) = 1$<br>e and φ(n) are co-prime |
| **5** | Determine (d):<br>$d \equiv e^{-1}(mod\varphi(n))$<br>(d) is the modular multiplicative inverse of e (modulo φ(n)). This is stated as solving the d given<br>$d.e \equiv 1(mod\varphi(n))$ |

*(e,n) is the public key*

*(d,n) is the private key*

**Table 2** DNA encoding rules

| Base | A | C | T | G |
|---|---|---|---|---|
| Rule 1 | 00 | 10 | 01 | 11 |
| Rule 2 | 00 | 01 | 10 | 11 |
| Rule 3 | 01 | 11 | 00 | 10 |
| Rule 4 | 01 | 00 | 11 | 10 |
| Rule 5 | 10 | 11 | 00 | 01 |
| Rule 6 | 10 | 00 | 11 | 01 |
| Rule 7 | 11 | 10 | 01 | 00 |
| Rule 8 | 11 | 01 | 10 | 00 |

### Encryption process

$$C = P^{e} mod(n)$$

### Decryption process

$$P = C^{d} mod(n)$$

where $P$ is the original data and $C$ is the cipher data.

## DNA cryptography

### DNA encoding

DNA computing in cryptography is a probable technology, which may bring new hope for creating unbreakable algorithms by utilizing DNA molecules in encoding. DNA strands consist of long polymers containing millions of nucleotides. Each nucleotide consists of four nitrogen bases (A,T,C,G), five-carbon sugar units, and a phosphate group.

In the cryptography concept, these four-letter alphabets (A, G, C, T) can be utilized to encode the secret information, that is enough or more for computer needs (only two digits) [14]. DNA cryptography is a promising technology due to the high speed of DNA computing, small power requirements, and minimal storage size as just one gram of DNA contains 1021 DNA bases that are equal to "108 TB" of data which can keep all the world data in only a few milligrams [15]. To encode the secret data into a DNA sequence, the binary secret data are converted according to one of the eight encoding rules as shown in Table 2.

To encode secret data in this study, the encrypted image has been encoded using rule 3 (p) (the key value) and the encrypted report has been encoded using rule 5 (q key value).

### DNA mixing

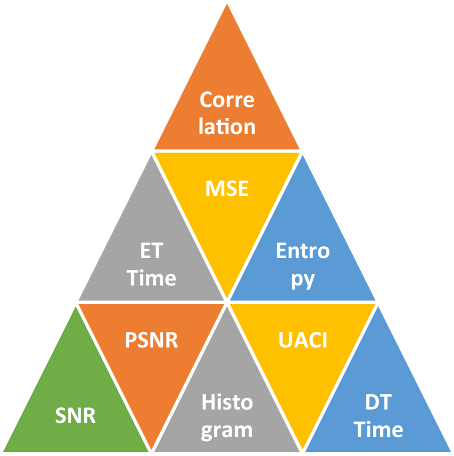
In this stage, both DNA strands from the encrypted image and the encrypted secret message have been mixed with percent (p/q), where p is the number of the public key and q represents the private key. The idea of using such percent is using the same used keys without increasing the secret parameters. The shown example explains the mixing idea between both strands with (p/q) present.

```
DNA_img=[x1,x2,x3,x4,x5,x6,x7,x8,...]              (for p=3)

DNA_msg=[y1,y2,y3y4,y5,y6,y7,y8,y9,y10,...]   (for q=5)

DNA_mix= [x1,x2, x3,y1,y2,y3, y4,y5,x4, x7,x8, y6, ,y7,y8,y9,y10]
```

### Evaluation metrics

Any cryptosystem presented should be evaluated to ensure its robustness and its efficiency in encrypting data, so different evaluation metrics have been presented for that purpose. In this study, some of them have been applied like correlation, histogram, signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR), encryption and decryption time (ET-DT), entropy, and mean square error (MSE). All these statistical metrics have been applied besides unified average changing intensity (UACI) which represents the difference between the average intensity between the plain and encrypted data. It can be calculated from [16]:

$$UACI = \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{F * T} * 100\% \tag{1}$$



## Results

Proposing a cryptosystem is not an easy process; it should be robust, fast, and yet secure. Therefore, a cryptosystem has been proposed in this study based on one of the most powerful cryptographic algorithms (RSA) which is supported by DNA computing theories for adding another security level to the proposed system. In this experiment, different images of different sizes, for MRI brain tumor images downloaded from Kaggle, are encrypted using the RSA algorithm with the public key encryption and then encoded into DNA format. Finally, this encrypted image is providing the feasibility of security to the image in network security. This experiment has been implemented on MATLAB 2018, Laptop Dell Core i7, RAM 8 GHz.

To evaluate our proposed scheme, we have used different evaluation metrics starting with the histogram of the encrypted and original data, insecure system should be completely different as shown in Fig. 3.

Figure 3 shows two brain images (normal–abnormal) and how its histogram differs completely from the histogram of encrypted images which indicates its security.

The second evaluation metric is the encryption and decryption time for each algorithm and after combining both as shown in Table 3.

The rest evaluation metric is the statistical measures which are summarized in Table 4.

Figure 4 shows the quality of some normal and abnormal images after and before encryption.

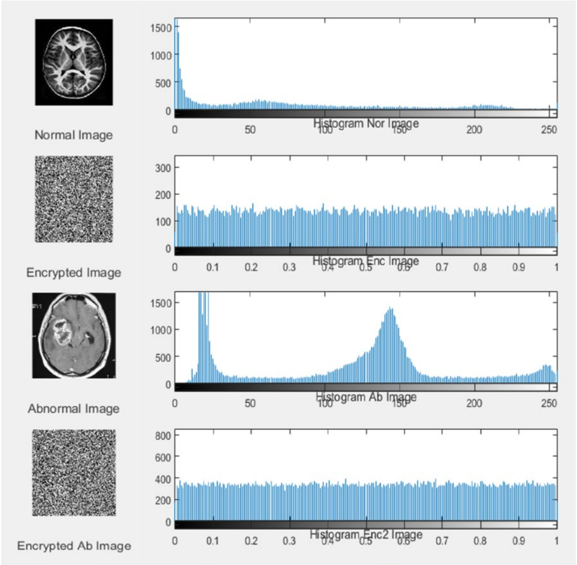


**Fig. 3** Histogram of normal and abnormal images and their encryption image

**Table 3** Encryption/decryption time for each algorithm in sec

| | **Report of 100 characters** | | **Image** | |
|---|---|---|---|---|
| | ***ET*** | ***DT*** | ***ET*** | ***DT*** |
| RSA | 0.162 | 0.128 | 16.641 | 13.766 |
| DNA encoding | 0.082 | 0.054 | 15.860 | 3.801 |
| Both | 0.228 | 0.202 | 31.329 | 18.472 |

ET, encryption time; DT, decryption time

**Table 4** Statistical evaluation metrics

| **Metric** | **Average values** |
|---|---|
| MSE | 1.3930e-04 |
| PSNR | 41.4396 |
| Entropy of the encrypted image | 0.7369 |
| Correlation | 0.85746 |
| UACI | 32.68 |
| SSIM | 0.9223 |
| SNR | 1.1134 |

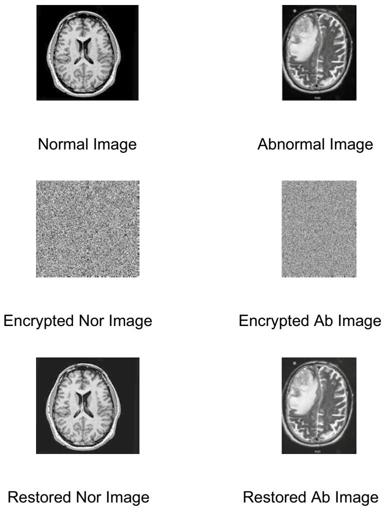


**Fig. 4** Normal and abnormal brain images after and before encryption

## Discussions

In the digital world, the security of medical images has become more important as the communication between global hospitals has increased rapidly. All the algorithms can be applied in real-time image encryption but find a low level of security. In this study, the image encryption algorithm proposed is efficient and highly securable with a high level of security and less computation. The results of the simulation show that the algorithm has advantages based on its techniques which are applied to images. Hence, it is concluded that the techniques are efficient for image encryption and give security in the public network. It is known that RSA is a fast and efficient algorithm, but here adding DNA cryptography enhances the security level of the proposed algorithm; also, the mixing process complicates the proposed system to increase its robustness that can be utilized safely in IoT technology.

Any slight difference causes a very big change in the results. This appears in two points: The first is in the process of decoding the mixture. If a change is made in the value of one of the keys, the resulting DNA is not expressive of the actual one, which greatly affects the results. As for the second, this change in the decryption process appears through the RSA algorithm, in which the wrong decryption leads to a change in the recovered data. This confirms the sensitivity of the keys used in this cryptosystem.

## Conclusions

RSA provides usually a highly secure data encryption system. Although cloud computing is a modern developing model, the attackers come with new eavesdrop techniques to extract secret data. So, the traditional algorithms should be supported with novel technologies like DNA cryptography as proposed in this study. DNA encoding rules have been used to increase the security level for the proposed system which proved its efficacy in this goal. In the future, adding another security level may be provided like chaotic maps.

### Abbreviations

AES: Advanced Encryption Standard; ATMs: Automated teller machine; DES: Digital Encryption Standard; DNA: Deoxyribonucleic acid; DoS: Denial of sleep; ET-DT: Encryption and decryption time; GUI: Graphical user interface; IoT: Internet of things; MRI: Magnetic resonance imaging; MSE: Mean square error; NPCR: Number of pixels change rate; PSNR: Peak signal-to-noise ratio; RSA: Rivest–Shamir–Adleman; SNR: Signal-to-noise ratio; SSIM: Structural similarity index measurements; TPRNG: True prime random number generator; UACI: Unified average changing intensity.

### Acknowledgements

Not applicable.

### Author contributions

The authors provided a novel framework for enhancing E-health security and IoT security and mixed RSA with DNA cryptography theory. The provided the novel idea of mixing two strands of DNA: the first strand represents the medical image and the second strand represents the medical report, and the mixing percent refers to the prime numbers (keys) used in RSA. All authors read and approved the final manuscript.

### Funding

No funding was received.

### Availability of data and materials

The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

## Declarations

### Ethics approval and consent to participate

Not applicable.

### Consent for publication

Not applicable.

### Competing interests

The authors declare that they have no competing interests.

### Author details

[1]Biomedical Engineering Department, Helwan University, Cairo, Egypt. [2]Biomedical Engineering Department, Misr University for Science and Technology, Cairo, Egypt. [3]Basic and Applied Science Department, Faculty of Engineering, Arab Academy of Science and Technology AASTMT, Cairo, Egypt.

Received: 22 August 2021 Accepted: 25 July 2022
Published online: 04 August 2022

### References

1. Tornea O (2013) Contributions to DNA cryptography: applications to text andimage secure transmission. PhD diss., Université Nice Sophia Antipolis; Universitatea tehnică (Cluj-Napoca, Roumanie)
2. Zhang Q (2021) An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption. In: 2021 2nd international conference on computing and data science (CDS), pp 616–622
3. IoT (Last seen: 2020). https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
4. Fotohi R, Yusefi M (2019) Securing wireless sensor networks against denial—of—sleep attacks using RSA cryptography algorithm and interlock protocol. Wiley, New York
5. Liu M, Ye G (2021) A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm. Math Biosci Eng 18:3887–3906
6. Al-Obeidi AS, Al-Azzawi S (2020) Hybrid synchronization of high-dimensional chaos with self-excited attractors. J Interdiscipl Math 23:1569–1584
7. Lin R, Li S (2021) An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm. Secur Commun Netw 2021
8. Mir UH et al (2022) Color image encryption using RSA cryptosystem with a chaotic map in Hartley domain. Inf Secur J A Global Perspect 31:49–63
9. Goshwe N (2013) Data encryption and decryption using RSA algorithm in a network environment. IJCSNS Int J Comput Sci Netw Secur 13
10. Kim Y (2020) New RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices. https://www.mdpi.com/journal/electronics, 2 February 2020
11. Raslau FD et al (2015) Memory part 2: the role of the medial temporal lobe. Am J Neuroradiol 36:846–849
12. Dataset (Last seen 2020). https://www.kaggle.com/navoneel/brain-mri-images-for-brain-tumor-detection.
13. Yousif SF (2018) Encryption and decryption of audio signal based on RSA algorithm. Int J Eng Technol Manag Res 5:57–64
14. Mondal M, Ray KS (2019) Review on DNA cryptography. arXiv preprint arXiv:1904.05528
15. Cryptography (Last seen 2020), "https://www.geeksforgeeks.org/dna-cryptography/."
16. Elamir MM et al (2021) Hybrid image encryption scheme for secure E-health systems. Netw Model Anal Health Inform Bioinform

## Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.