SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I11P107

Volume 11 Issue 11, 62-78, November 2024

Original Article

Lightweight Signcryption Scheme Using Improved SIMON and Ring Signature for Medical Image Security

Afreen Fatima Mohammed[1,2], Syed Shabbeer Ahmad[3]

[1]*Department of CSE, University College of Engineering, Osmania University, Telangana, India.*
[2]*Department of Emerging Technology (Data Science), CVR College of Engineering, Telangana, India.*
[3]*Department of CSE, Muffakham Jah College of Engineering and Technology, Telangana, India.*

[1]*Corresponding Author : afreen0422@gmail.com*

Received: 08 September 2024 Revised: 07 October 2024 Accepted: 06 November 2024 Published: 03 December 2024

Abstract *- A Lightweight Signcryption scheme using Improved SIMON and Ring Signature for medical image security is proposed in the paper. As medical images in the healthcare sector have a greater security concern, this paper aims to propose a signcryption scheme that would apply encryption and signature in a single step, thereby providing confidentiality and authentication. The major aim is to provide security to the medical images in the healthcare sector, such as X-ray, MRI, and CT scan images. Applying a proper security mechanism can secure these images of the patients. The proposed signcryption process applies a lightweight encryption SIMON algorithm for encryption and a ring signature for authentication. The proposed signcryption process guarantees the image's confidentiality and the sender's identity. The proposed method is implemented using the python platform, and results are compared with existing methods. Two different datasets have been used to evaluate the performance of the proposed scheme. The simulation outcomes demonstrate the proposed approach's effectiveness in boosting the security and proficiency of medical data transmission.*

Keywords *- Decryption, Encryption, Lightweight, Ring signature, Signcryption.*

1. Introduction

Digital imaging technology plays a significant role in diagnosing diseases in the medical system. The privacy and security of health-related applications are currently challenging due to technological developments in the healthcare sector [1-3]. Medical informatics systems regard medical images as important and sensitive data. Secure encryption and authentication techniques must be designed to transmit medical images across an open medium. One of the most efficient solutions to achieving security is through encryption. The need to secure the confidentiality and integrity of medical images has grown in tandem with using these images in healthcare.

A patient's medical records, which may include private information, are essential for diagnosis, treatment planning, and follow-up care. However, significant risks are associated with sending and storing these images across networks that may not be secure. These risks include data manipulation, privacy breaches, and illegal access. To overcome these obstacles, medical image security relies on cryptographic methods to keep pictures private, original, and unaltered at all times. One of the most effective methods for protecting medical images is Signcryption. Signcryption is defined as a cryptographic primitive that combines encryption with digital signatures.

Signcryption ensures the security of medical images by signing them to verify their validity and integrity and encrypting them to maintain their confidentiality. Due to the essential requirement of securing and upholding the confidentiality of all patient-related information, this dual capability assumes great significance in a healthcare setting. Recently, a lot of work has been done to make signcryption techniques more secure and efficient. One way to protect medical pictures is to combine signcryption with the National Security Agency's (NSA) SIMON lightweight block cipher. Mobile and embedded systems, prevalent in healthcare settings and known for their limited resources, are ideal for SIMON's efficiency and simplicity [4]. While the typical SIMON algorithm is efficient, it does have several flaws that smart attackers may exploit. As a means of reducing these risks, researchers have proposed a new version of the SIMON algorithm that is both lightweight and more resistant to cryptanalysis attacks. To further improve medical image security, the signcryption method uses ring signatures in addition to an upgraded SIMON algorithm. A ring signature is a digital signature that allows data to be signed by a group member without revealing which specific member has signed it. In 2001, Rivest, Shamir, and Tauman invented a ring signature. Ring signature enables an individual to anonymously sign a message on behalf of a group [5, 33].

There has been a research gap in integrating ring signatures with lightweight cryptographic algorithms. The problem is identifying the ring signature mechanism, which makes the signer anonymous and provides confidentiality to the data. This paper addresses the mechanism of integrating ring signatures with cryptographic algorithms.

Ring signature is particularly useful in healthcare organizations where the confidentiality of the signature, whether a doctor or a medical technician, is of the utmost importance. Signcryption systems employ ring signatures to keep the signatory's identity secret while securely transmitting and authenticating the medical image. This extra safeguard becomes paramount when it's critical to protect the identities of both patients and healthcare providers.

Combining an improved SIMON algorithm and ring signature-based signcryption establishes a robust foundation for medical image security. This method solves important problems with healthcare data security by providing powerful signature methods to guarantee the validity and integrity of the images, as well as strong encryption to prevent unwanted access to critical medical images [6-8]. In addition, medical imaging systems may continue to function efficiently even with strict security measures in place because of the SIMON algorithm's small footprint, which makes it a beneficial choice for settings with limited resources. The importance of trustworthy cryptographic solutions is increasing due to healthcare systems' growing dependence on digital technology. Medical image security has long been an issue. However, a new signcryption technique combining enhanced SIMON signatures with ring signatures provides a complete solution that strikes a satisfactory balance between efficiency, authenticity, and secrecy for protecting sensitive medical data.

The proposed work contributes to a unique scheme for secure medical image transmission. This evolution is intended to make it difficult for any assailant to interpret any encoded image without a given secret key. The proposed scheme employs a lightweight encryption algorithm in the IoT Context, which has proven useful in safeguarding healthcare data in transit, especially in transmitting medical images.

2. Related Work

In the last few years, many signcryption schemes have been proposed for different applications. A study [9] proposed a novel medical image signcryption scheme that employs hybrid cryptography. It uses the elliptic curve cryptographic algorithm to generate secret encryption keys for signcryption and chaotic maps to encrypt medical images [34]. The proposed image signcryption scheme claims to provide confidentiality, authentication, integrity, unforgeability, forward secrecy, and non-repudiation but introduces complexity while encrypting an image using a chaotic map [35]. In [30], authors suggested an attribute encryption method for providing security to patients' health records but failed to address the authentication mechanism. In [31], the author addresses the authentication mechanism for IoT devices.

In [10], the researchers introduced sign encryption which is a certificate in nature that protects users from within the organization and also achieves forward secrecy and non-repudiation. In [11], the authors described the identity-based signcryption scheme and how knowing the public key is not a problem since it is easy to identify key strings protected by a trusted authority that generates that particular string private key from several system-specified master keys. In [12], the authors describe an identity-based ring signcryption scheme that allows for both the privacy and the authentication of a certain group of users communicating over a mobile ad-hoc network such as Bluetooth. A bilinear pairing-based verifiable certificates ring signcryption scheme is employed [36]. In [13], the scheme allows the sender to send messages while keeping the privacy and authenticity of the messages and the sender himself. It shows that it works in the random oracle model [36]. In [14], generalized ring signcryption is described as allowing the usage of a single key pair and having a combining algorithm to perform both the ring signature and the ring signcryption operations. This approach is ideal for scenarios with a large user base, limited storage capacity, or evolving function requirements.

In [15], the authors introduced a novel identity-based ring signcryption scheme that relies on pairings, thereby exposing its vulnerability to various security threats. An ECC image signcryption scheme resulted in less power consumption and minimal computational cost [16]. The authors of [17] proposed a method of outsourced attribute-based signcryption using blockchain resources for the secure distribution of emails containing Electronic Health Records (EHR) in the cloud with multiple verifiable trusted third parties [39]. This system guarantees the privacy and insecurity of electronic health record systems and the confidentiality of health record signers while also relieving the user’s processing strain owing to a verifiable outsourcing computation system [32]. In [18], the author proposed another solution, this time regarding e-prescription systems, which is simple, not heavy and above all, secure, being based on hyperelliptic curve proxy signcryption [18]. Compared to other schemes, it saves time and money on both computing and communication.

3. Proposed Model

This paper proposes an improved SIMON and ring signature scheme that combines the cryptography features of the ring signature and SIMON block cipher to provide lightweight encryption and authentication. We apply an ECC-based ring signature to the digital signature. The SIMON block cipher provides reliable and secure cryptography primitives suitable for resource-constrained circumstances and the source for encryption and decryption operations.

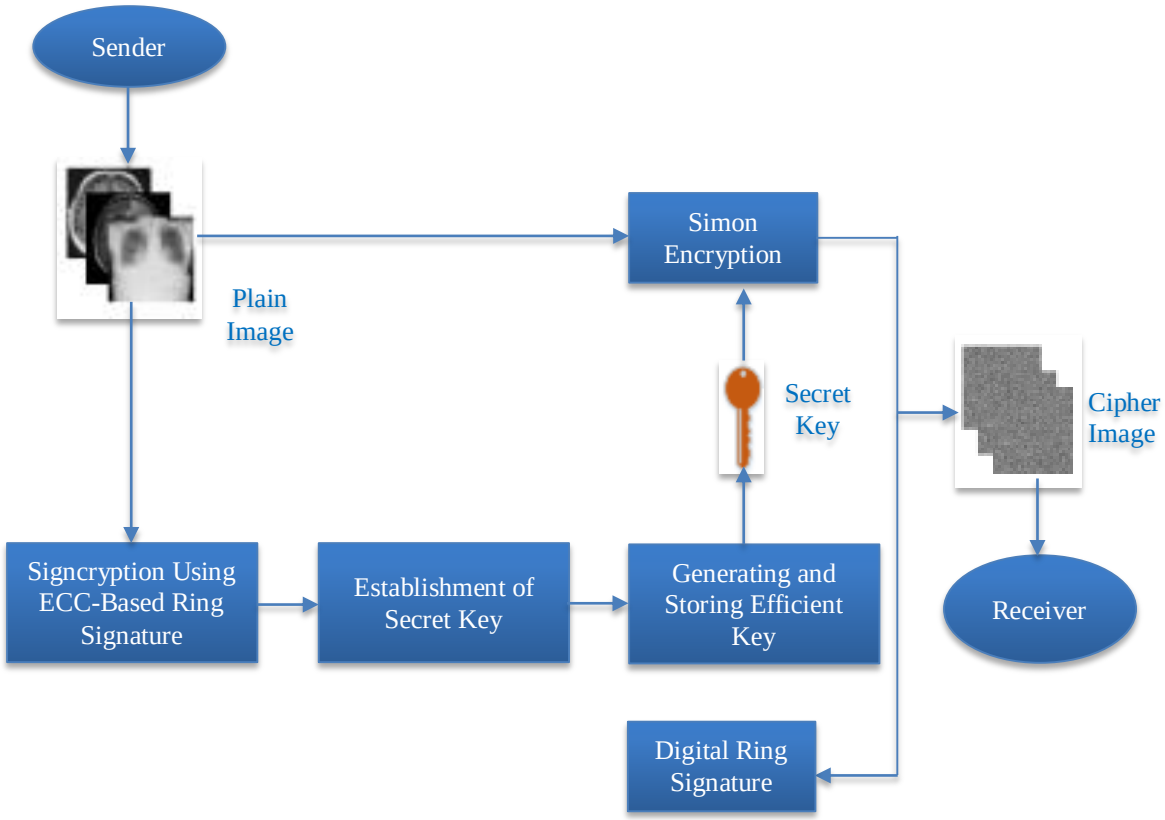


Fig. 1 Block diagram of ISRS

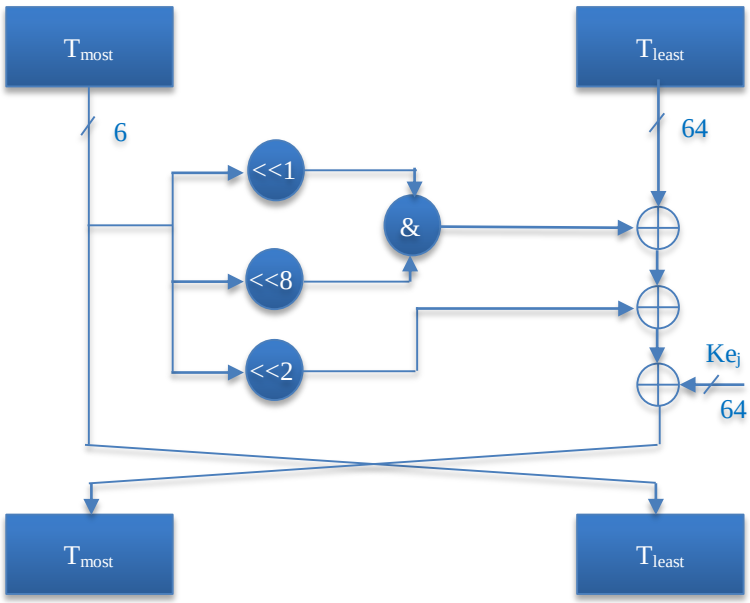


Fig. 2 SIMON encryption

3.1. SIMON Encryption

A key scheduling process is applied to generate another key for each SIMON algorithm's encryption round. The key scheduling process applies some logical operations such as XOR, AND and left circular shift arithmetic logic. The proposed method utilizes the SIMON 128/128 configuration, offering a security level comparable to AES-128 for secure image transmission [19]. As shown in Figure 2, the round function and key expansion function are SIMON encryption's two main components.

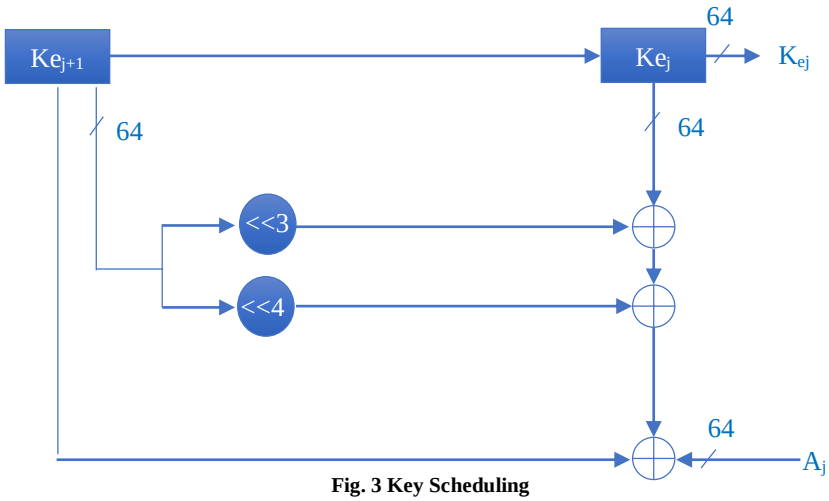


Fig. 3 Key Scheduling

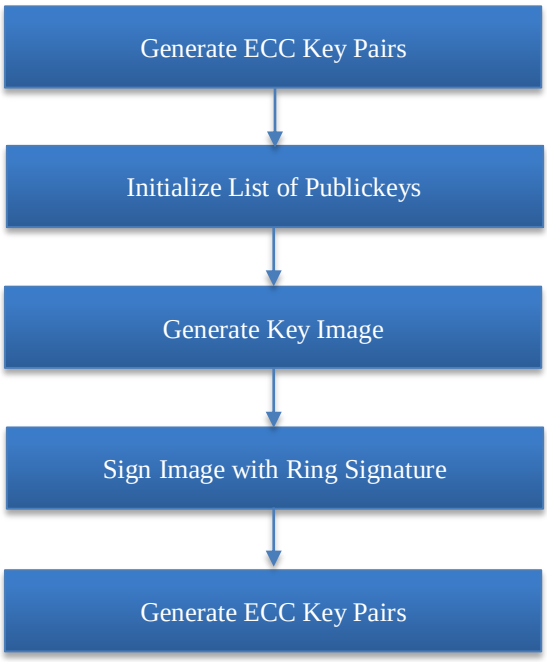


Fig. 4 Flowchart of generating and verifying ring signature

The key scheduling process, called the key generation process, is applied to the SIMON encryption algorithm. In every cycle, this process is employed to find the value of the key. Each operating round of encryption uses a different key. Figure 3 demonstrates the SIMON key scheduling process. It uses XOR logic and performs two shift-right operations: shift-right three and shift-right four. The function responsible for generating keys makes most of the 64 bits available to logic operations, and the 64 mask bits are combined with the output mask to which the 64 round constant is XORed. A variable known in this paper as a round constant is regarded as a constant that is determined at the design stage and optimized for each particular configuration. Three (3) 64-bit XOR operators and two (2) 64-bit shift operators (shift right three and shift right four) are used [37].

By applying a 128-bit key and a 128-bit plain image, the encryption scheme creates a 128-bit cipher image. The round function applies logical operations on the most significant 64-bit T_{most} - the upper half block of the plain image, then Xor-ed with the round key K_{ej} and the least significant 64-bit T_{least} - the bottom half block of the plain image [37]. The blocks contain the input image and the key in some combination, and at the end of the round, the newly generated images are written into the top block, and the whole top block image is moved down. The list contains only a general description of SIMON, clarifying that it consists of 68 cycles. Each cycle features a SIMON round operation during which three 64-bit shift operations are carried out: shift left one, shift left two, and shift left eight, as well as three 64-bit XOR operations and one 64-bit AND operation [38].

Figure 4 depicts the flowchart for generating and verifying ring signatures.

3.2. Authentication Using ECC-Based Digital Ring Signature

By leveraging ECC-based digital ring signatures, healthcare providers can uphold the integrity and authenticity of transmitted medical images while respecting the anonymity of signers within the group, thereby fostering secure and confidential communication in medical environments. A ring signature is a group signature that utilizes several public keys rather than just one key [20, 21]. The ring signature hides the signer's identity from the verifier. The signature authenticates the medical image being sent by ensuring that the image is an authenicated image sent by someone who is an authorised user in the group by hiding the details of the user who has signed an image. Ring signatures, in contrast to other group signatures, do not require a manager or any other form of cooperation between the members. Three components, KeyGen (), Sign () and Verify () make up a basic ring signature.

3.2.1. KeyGen ()

Each user submits a security parameter (l), which is used to produce a two-part key designated as (PubK PrK), namely the public key and the private key, respectively. The utilized approach incorporates the ECC algorithm [22] to create the signature generation necessary for private and public keys. Elliptic curves can produce various public and private key pairs. The elliptic curve, defined over a field, produces key pairs that serve as the private and public keys for signature generation.

3.2.2. Sign ()

The procedure employs the private key *PrK* of a certain member of the ring, the public key set $l = \{PubK_1, PubK_2, ..., PubK_p\}$ of the selected members of the ring, and the target signature to generate a signature for the message *M*. In accordance with specific rules, one of the parameters in the signature follows a ring.

3.2.3. Verify ()

This algorithm functions as a deterministic algorithm, takes the message *M* and the public key set $l = \{PubK1, PubK2, \ldots, PubKp\}$, and signature as input. If the verification is successful, it outputs "accept"; otherwise, it outputs "reject.".

Algorithm to generate ECC Key Pairs

Step : 1 Select elliptic curve SECP256R1
Step : 2 Generate private key using a cryptographic primitive ec.generate_private_key(SECP256R1,default_backend)
Step : 3 Derive the public key from the generated private key using private_key.public_key()
Step : 4 Return the tuple (private_key, public_key)

Algorithm Generate_Key_Image

HKDF is a Hash-based Message Authentication Code based Extract-and-Expand Key Derivation Function applied to generate key images.

Step : 1 Input: private_key, public_key
Step : 2 Compute shared_secret = private_key.exchange(ECDH, public_key)
Step : 3 Initialize HKDF with:
- Algorithm: SHA-256
- Length: 32 bytes
- Salt: None
- Info: 'key_image'
- Backend: default_backend()
Step : 4 Derive key_image using HKDF from shared_secret

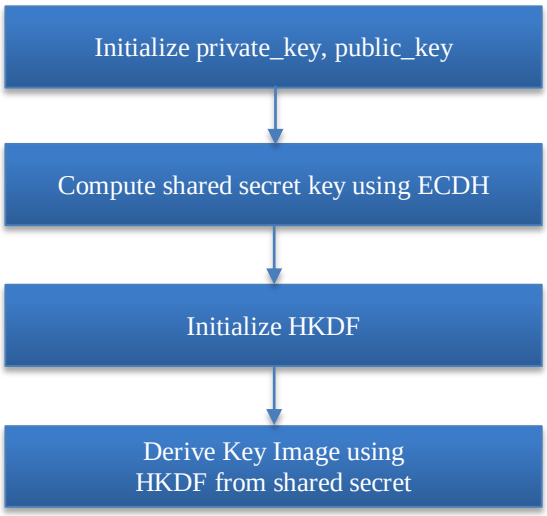


Fig. 5 Flowchart to generate key image

Algorithm to Sign Image with Ring Signature

1. Prepare Input Data:
Image: The medical image to be authorised.
Private Key: The private key is used to sign the image for authorisation.
Public Keys: A list of public keys that form the ring, one of which is the key of the private key.
2. Generate Key Image:
Step 2.1: Use the private key and its corresponding public key to generate a key image.
Step 2.2: This key image is a unique identifier for the private key within the ring.
3. Initialize Signature Collection:
Step 3.1: Create an empty list named signatures to store the key image and individual signatures.
4. Sign for Each Public Key in the Ring:
Step 4.1: Iterate through each public key in the list public_keys:
Step 4.1.1: For the current index i, check if the current public key matches the public key derived from the private_key.
If True:
Step 4.1.1.1: Append the previously generated key image to the signatures list.

If False:
Step 4.1.2: Generate a unique nonce:
Step 4.1.2.1: Use a Key Derivation Function (HKDF) with a unique identifier (e.g., index i) to derive a 32-byte nonce.
Step 4.1.3: Prepare data for signing:
Step 4.1.3.1: Concatenate the message, key_image, and the generated nonce into a single string.
Step 4.1.4: Sign the concatenated string:
Step 4.1.4.1: Use the private_key to sign the concatenated string with the Elliptic Curve Digital Signature Algorithm (ECDSA) using SHA256.
Step 4.1.5: Append the resulting signature to the signatures list.
5. Return the Ring Signature:
Step 5.1: Return a list containing:
Step 5.1.1: The key image.
Step 5.1.2: All the individual signatures are generated in step 4.

Algorithm to Verify Ring Signature
1. Extract Components from Signature:
Step 1.1: Extract the key image from the first element of the signature list.
Step 1.2: Extract the actual signatures from the remaining elements of the signature list.
2. Determine the Number of Public Keys:
Step 2.1: Calculate the number of public keys in the public_keys list.
3. Verify Each Signature:
Step 3.1: Iterate through each index i and corresponding public_key in the public_keys list:
Step 3.1.1: Generate the nonce for the current index i using the format f'nonce_{i}'.encode().
Step 3.1.2: Check if the current public_key matches the i-th public key in the public_keys list.
If True: Skip the verification for this public key, as it corresponds to the key image used during signing.
If False:
Step 3.1.3: Create a verifier object for the current public_key using the signature at index i and ECDSA with SHA256.
Step 3.1.4: Concatenate the message, key_image, and nonce to form the data to be verified.
Step 3.1.5: Update the verifier with the concatenated data.
Step 3.1.6: Attempt to verify the signature:
If verification Fails: Return False immediately, indicating that the signature is invalid.
If verification Succeeds: Continue to the next public key.
Return Verification Result:
Step 4.1: If all signatures have been verified successfully, return True.

Figure 6 depicts the verification process of the ring signature. Figure 7 depicts the flowchart of the signing image with the ring signature, and Figure 8 illustrates the flowchart for verifying the ring signature. Ring signature is designed to be created upon the combination of the private key of the signer and the public keys of other group members; therefore, any group member could possibly have created the signature. Later, to avoid revealing the actual identity of the sender, the signed image and the digital ring signature are transmitted, and upon receipt, the recipient verifies the digital ring signature using the public keys. Successful verification not only confirms the authenticity and integrity of an image but also underlines its endorsement by a designated group member.

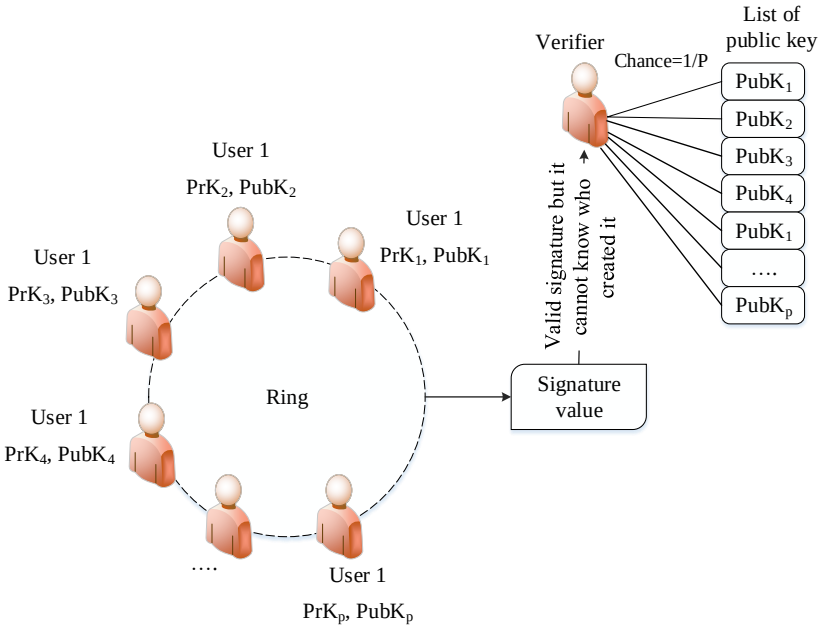


Fig. 6 Verification process of ring signature

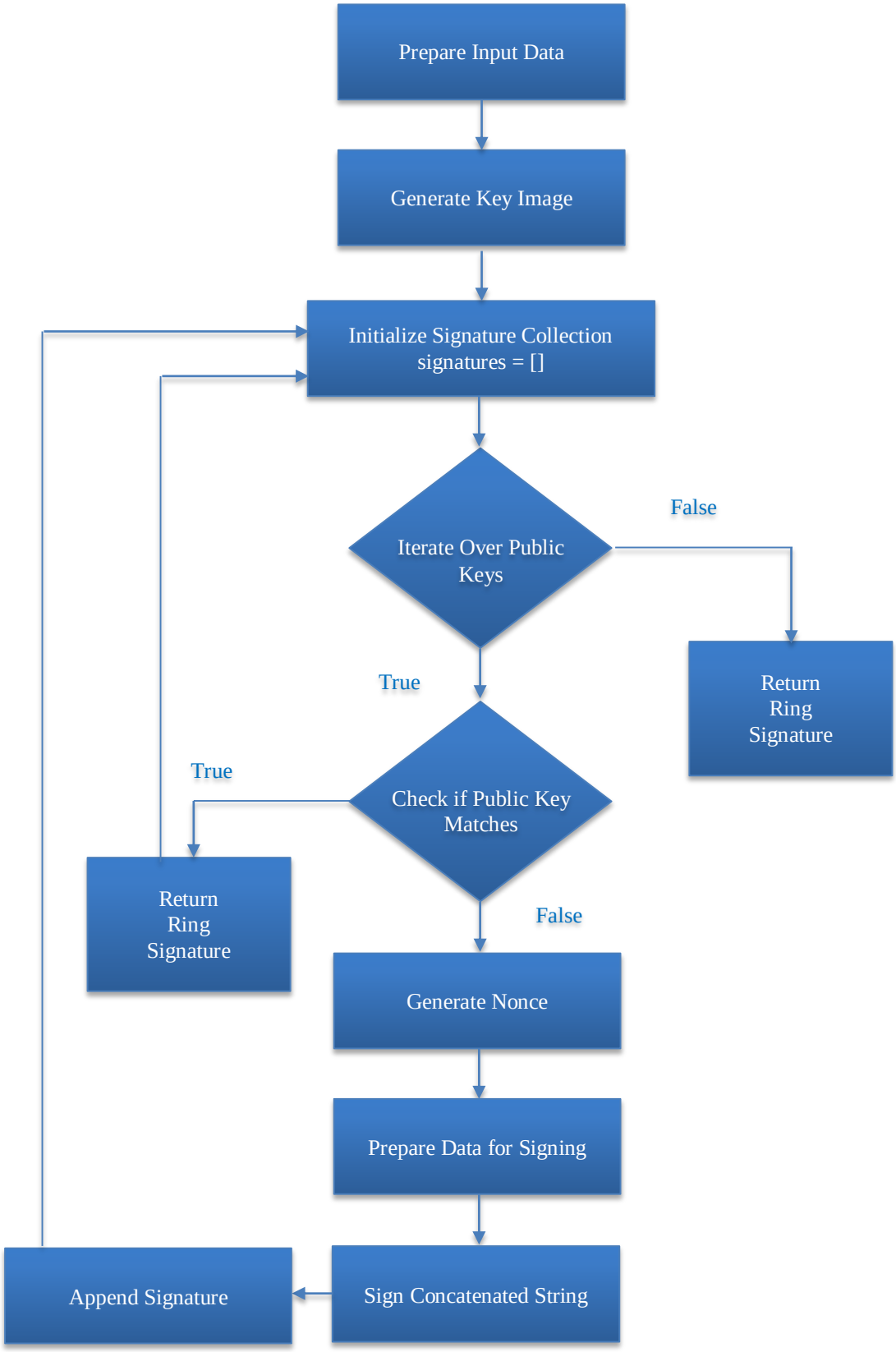


Fig. 7 Flowchart of signing image with a ring signature

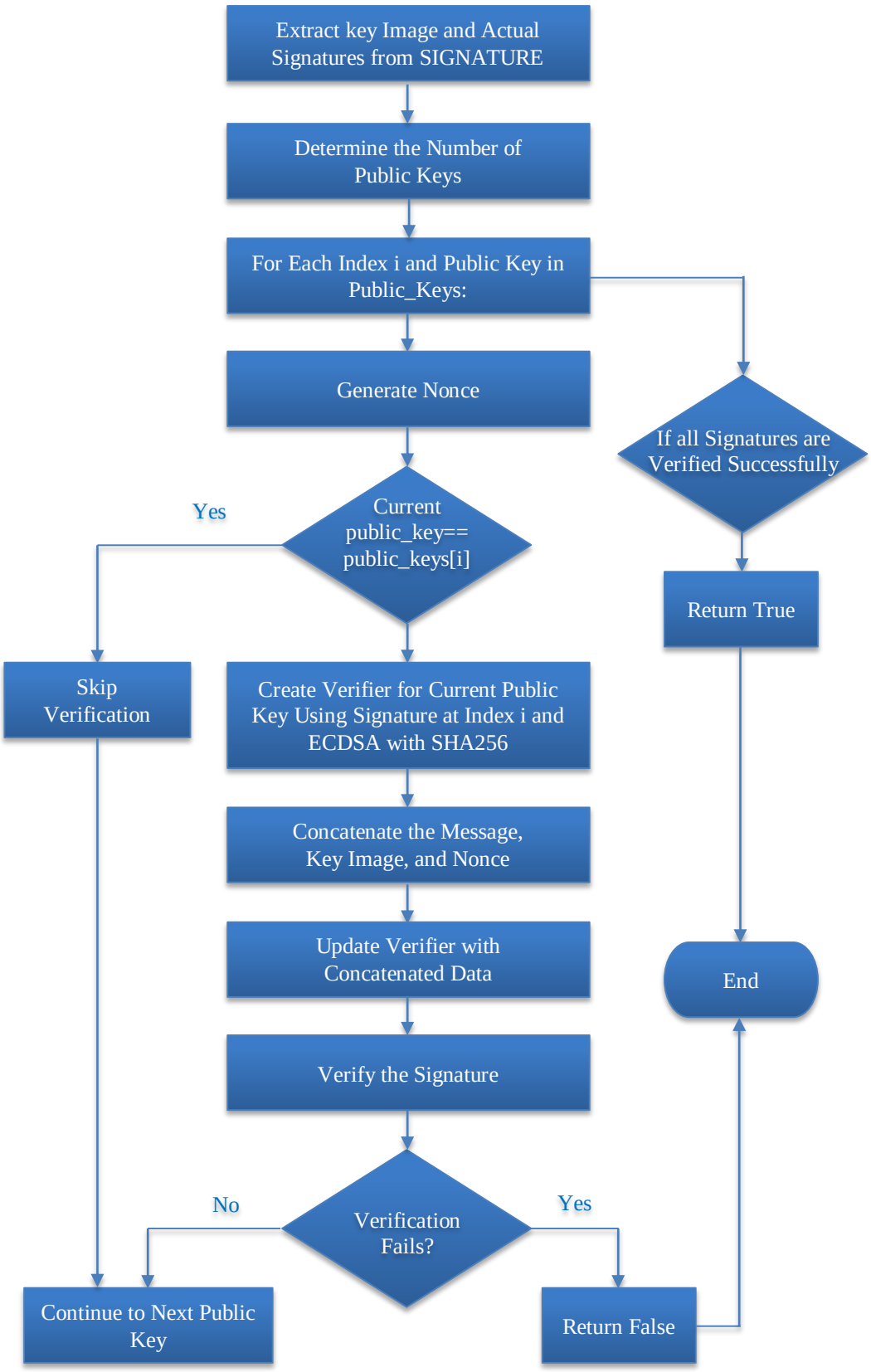


Fig. 8 Flowchart of verifying ring signature

4. Experimental Setup

4.1. Dataset

For analysis, the proposed method is implemented on a Python platform by utilizing two different medical datasets, the MRI brain tumor dataset [23] and COVID-19 X-ray dataset [24]. There are many medical datasets available on Kaggle and Git Hub.

However, two different medical datasets were used in the experiment conducted in this research. One of the datasets includes MRI scans of the human brain, while the other dataset contains X-ray images of patients afflicted with COVID-19. Figure 4(a-b) refers to the set of images taken from the stated two datasets.

4.2. Results and Performance Analysis

The proposed medical image signcryption method is tested using two different datasets separately, comprised of the MRI brain tumor dataset [23] and the COVID-19 X-ray dataset [24]. Next, the suggested strategy is applied to medical data using the 64-bit Python platform. The proposed approach is versatile enough to handle varying sizes and classes of medical images. Figure 4 displays images extracted from both datasets.

4.2.1. Baseline Methods

We use three different cryptographic methods for encryption: SPECK, Blowfish, and the Tiny Encryption Algorithm (TEA).

TEA

Tiny Encryption Algorithm (TEA) is an efficient and straightforward symmetric key block cipher. The TEA algorithm encrypts and decrypts data in 64-bit chunks. We split the 128-bit key into four 32-bit halves. Fixing the key size achieves a compromise between ease of use and security. The standard implementation uses 64 rounds of encryption, which can be adjusted to meet different security requirements [25]. More rounds improve security in most cases, but they might lower performance.

Blowfish

Blowfish is a block cipher that uses symmetric keys. The designers identified a need for a secure, versatile, and speedy replacement for the long-standing Data Encryption Standard (DES). In Blowfish, the key size may be anything from 32 bits up to 448 bits. Because of its scalability, customers may tailor the key length to their own requirements, striking a balance between security and speed. With 16 rounds of encryption, it is secure [26]. Substitution based on keys and permutation are two of the many intricate procedures that make up each round.

SPECK

The NSA developed a series of block ciphers called SPECK, which are lightweight. Tailored for constrained environments such as embedded devices and the Internet of Things (IoT), it is a partner cipher with another lightweight encryption scheme called SIMON. Regarding software, SPECK is performance-tuned, providing an excellent compromise between efficiency and security. SPECK allows users to select from 32, 48, 64, 96, or 128 bits as block size, determining the amount of data that can be encrypted or decrypted in a single operation [27]. A range of 64 bits to 256 bits is available. In addition, the size of the key depends on the block size in a modulo sense. A range of 64 bits to 256 bits is available.

Lattice-Based Signcryption

"Lattice-based Signcryption," an approach to cryptography, combines the features of digital signatures with encryption. This is a potential post-quantum cryptography option due to its imperviousness to quantum computer attacks. LWE and related lattice issues commonly serve as the foundation for lattice-based signcryption methods.

The key generation phase, which generates the sender and recipient's public and private keys, is a crucial component of any lattice-based signcryption method.

In the process of signing, the message gets transformed into a ciphertext which entails the use of a private key of the sender and a public key of the intended recipient for the encryption and decryption of the message sent. The final step is referred to as unsigncryption, which seeks to decode the message and check its authenticity using the encoded message, the receiving party’s private key and the sending party’s public key.

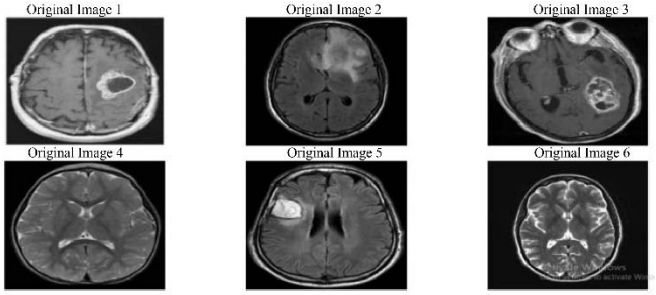
Quotable-Based Signcryption

This cryptographic approach combines the ideas of "quotability" with signcryption, a way that encrypts and digitally signs data simultaneously. The fundamental principle of quotable-based signcryption is that even if a third party did not get the original signed and encrypted communication, they may still be able to verify the integrity and validity of the quoted sections by simply extracting them. Quotable-based sign encryption is a versatile tool for secure and adaptable data exchange. It combines authenticity and secrecy in one quick process.

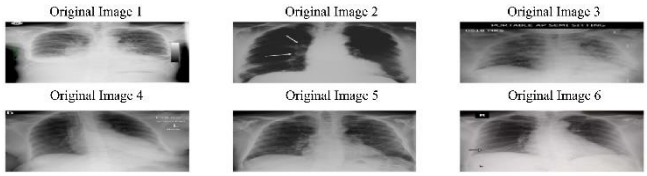
4.2.2. Histogram Analysis of MRI Brain Tumor and COVID-19 X-Ray Images

Medical imaging, such as X-ray images of COVID-19 or MRI brain tumors, heavily relies on histogram analysis, a fundamental method in image processing in general. It may aid in the differentiation of normal from pathological tissues by revealing the distribution of pixel intensities within an image.

Figure 9(a) represents the MRI images of the brain taken from the MRI brain tumor dataset, and the COVID-19 X-ray images of the chest from the COVID-19 X-ray dataset are depicted in Figure 9 (b).



(a) MRI brain tumor dataset



(b) COVID-19 X-ray dataset

Fig. 9 (a-b) MRI brain tumour and COVID-19 x-ray images

Figure 10 (a-b) shows the original images' histograms, whereas Figure 11 (a-b) shows the encrypted image histograms corresponding to them. Each picture should calculate the histogram, which displays the frequency of each intensity level. In the case of an 8-bit image, the intensity levels between 0 and 255 are displayed on the X-axis, and on the Y-axis, the count of each intensity is displayed. The tumor area on an MRI of the brain may appear as a sharp peak or change in intensity when contrasted with normal brain tissue. Compared to regular lung X-rays, COVID-19 X-rays may show a wider or skewed histogram due to infected areas.

4.2.3. Correlation Analysis of MRI of Brain Tumor and X-Ray Images of COVID-19 Patients

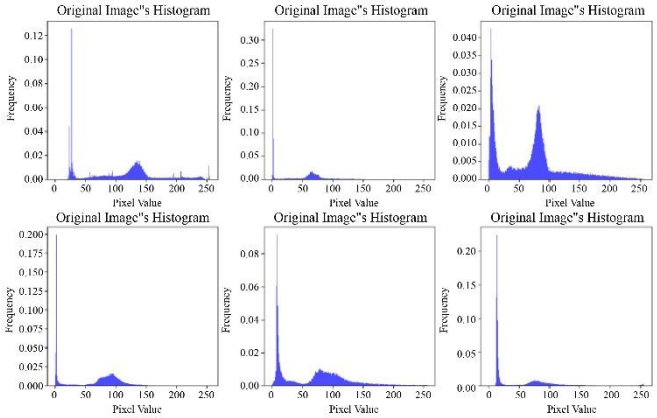
One of the potential applications of X-ray images obtained from patients diagnosed with COVID-19 and high-grade MRI scans of brain tumours is the analysis of common patterns and relations in both types of clinical pictures. The aim is to verify the existence of highly confused and diffused features by assessing the similarity between the plain image and the encrypted version of the image based on the correlation of the adjacent pixels. An effort is made to determine the correlation coefficients in the horizontal, vertical, and diagonal planes. Additionally, the connection between neighboring pixels is examined in Figure 12 (a-b).

4.2.4. Analysis of Computational Overhead in Terms of Encryption, Decryption, Signcryption and Designcryption Time

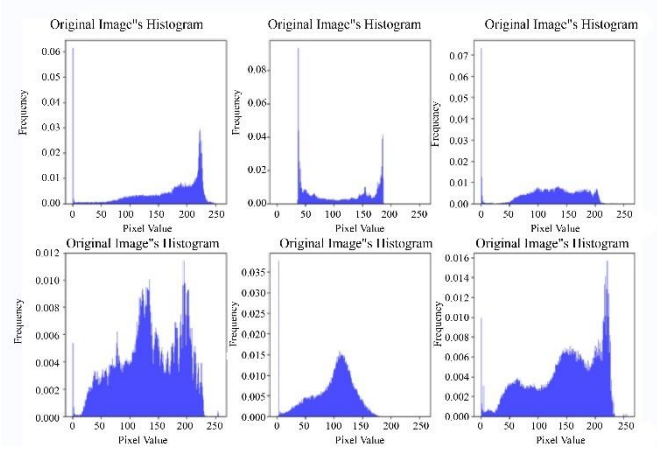
Computational overhead is analysed regarding the time taken to encrypt, decrypt, signcrypt and designcrypt. Table 1 gives the analysis of the time required for encryption and decryption in milli seconds [42]. A comparison of the encryption and decryption time of the proposed method is done with Tiny, Blowfish and SPECK lightweight encryption algorithms. The encryption time has been evaluated to 10.6133 milliseconds and decryption time to 10.3342 milliseconds for MRI brain tumor data set image and 10.4083 milli seconds encryption time and 10.41 seconds decryption time from COVID 19 X-ray dataset, which is lesser comparatively to other lightweight encryption algorithms. Similarly, Signcryption and Designcryption time is evaluated as shown in Table 2. Table 2 lists the other signature mechanisms, such as the Lattice-based method [28] and the Quatable method [29]. Figure 13(a-d) compares encryption time, decryption time, signcryption time and designcryption time using two datasets.

Table 1. Analysis of encryption and decryption time

MRI Brain Tumor Dataset		COVID 19 X-Ray Dataset	
Encryption Time (ms)	**Decryption Time (ms)**	**Encryption Time (ms)**	**Decryption Time (ms)**
11.1139	11.3776	11.4852	11.0458
11.2095	10.6025	11.2440	10.8553
10.6374	10.4143	10.7867	10.4578
10.6133	10.3342	10.4083	10.41



(a) MRI brain tumor dataset

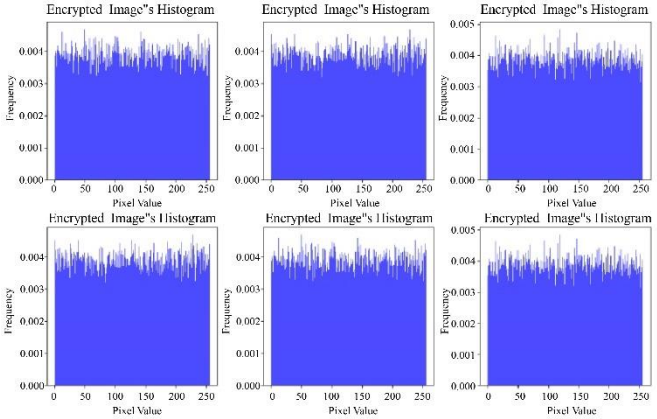


(b) COVID-19 X-ray dataset

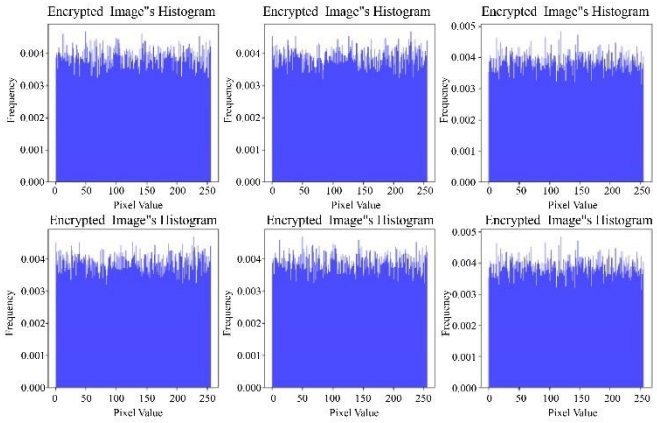
Fig. 10(a-b) Histogram analysis (original image)

Table 2. Analysis of Signcryption and Designcryption Time

Methods	MRI Brain Tumor Dataset		COVID-19 X-Ray Dataset	
	Signcryption Time (ms)	Designcryption Time (ms)	Signcryption Time (ms)	Designcryption Time (ms)
Lattice-Based Method	89.240	76.4406	98.4853	80.9088
Quatable-Based Method	71.161	67.0128	85.3731	84.4361
Proposed	20.282	13.4685	24.2140	10.6749

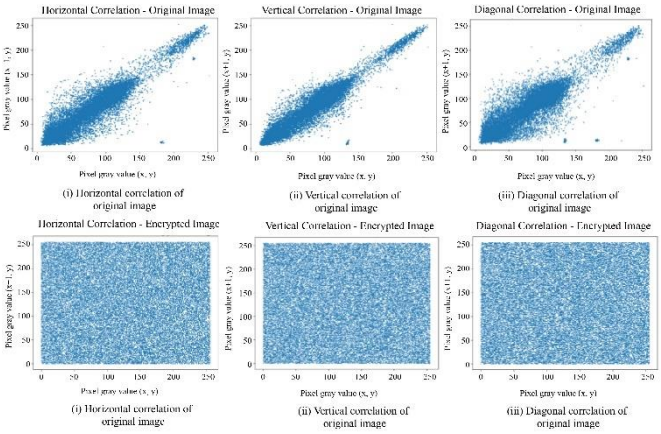


(a) MRI brain tumor dataset

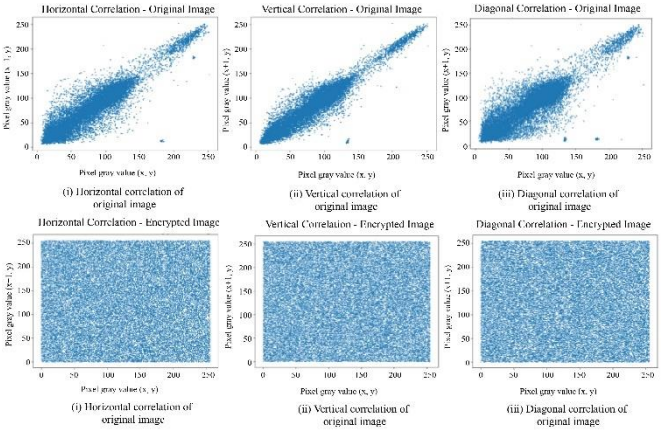


(b) COVID-19 X-ray dataset

Fig. 11(a-b) Histogram analysis (encrypted image)

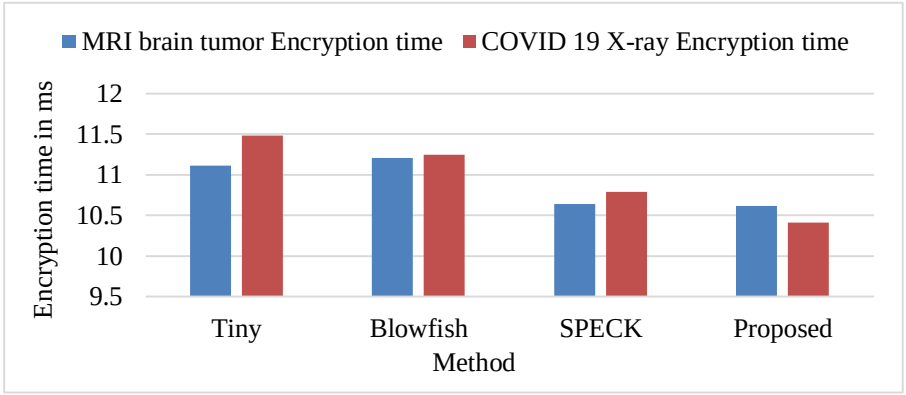


(a) MRI brain tumor dataset

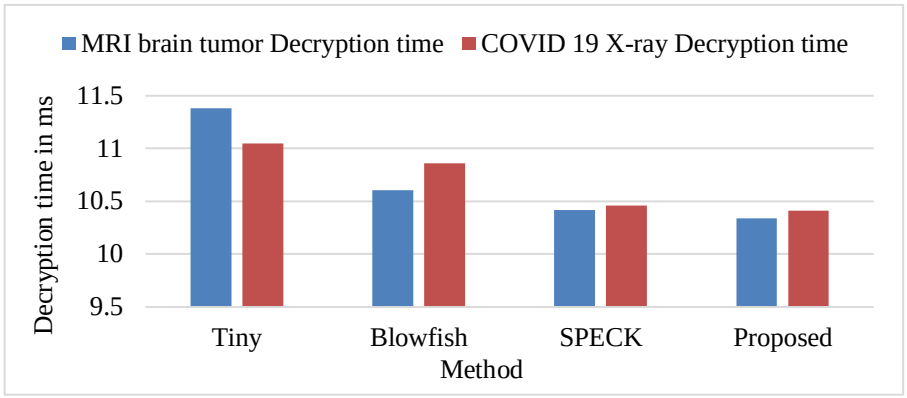


(b) COVID-19 X-ray dataset

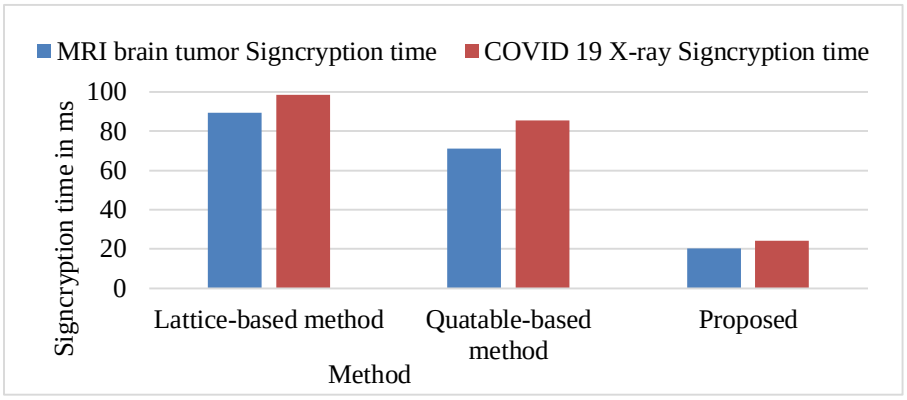
Fig. 12 (a-b) Correlation of adjacent pixels in unencrypted and encrypted image



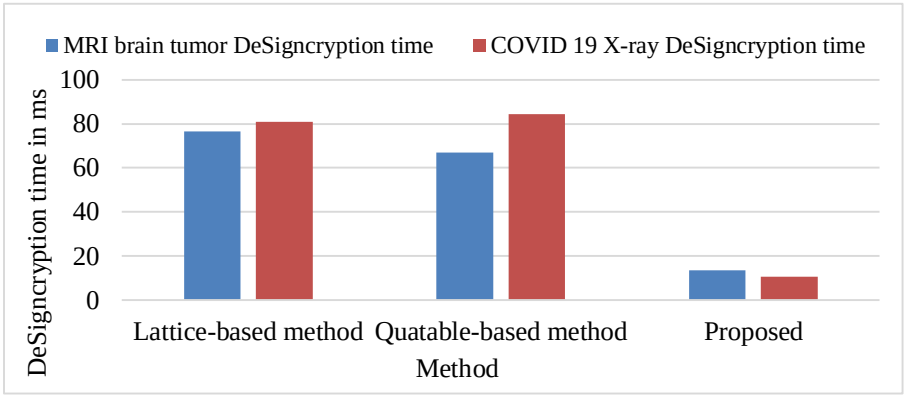
(a)



(b)



(c)



(d)

Fig. 13 (a-d) Analysis of comparison of encryption time, decryption time, signcryption time and designcryption time using two datasets

Table 3 and Table 4 list the performance analyses of the COVID-19 X-ray dataset and MRI brain tumor dataset for the proposed system.

4.3. Differential Attack Analysis

Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) are, therefore, assisting re-evaluation metrics that illustrate the extent to which a cipher image may endure attacks [40]. The proposed scheme is applied in various attacks to encode the original medical image while making minor adjustments. The two prior and subsequent encrypted images are related to obtaining a feasible association among the original encrypted images. UACI and NPCR applied quantitative parameters to measure the effectiveness of the encryption algorithm more precisely in the image encryption technique. The mathematical expressions of UACI and NPCR are presented in Equations (1) to (3) as:

$$UACI = \frac{\sum_{j=1}^{P}\sum_{k=1}^{N}|B_1(y,z) - B_2(y,z)|}{255 \times P \times N} \times 100\% \quad (1)$$

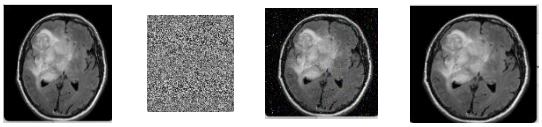
$$NPCR = \frac{\sum_{j=1}^{P}\sum_{k=1}^{N} E(y,z)}{P \times N} \times 100\% \quad (2)$$

$$E(y,z) = \begin{cases} 0 & if \ B_1(y,z) = B_2(y,z) \\ 1 & if \ B_1(y,z) \neq B_2(y,z) \end{cases} \quad (3)$$

Where, P represents the height, and N represents the width. B_1 and B_2 represent the two digital image with unique pixel variance. $P \times N$ represents the encrypted image size, B_1 demonstrates the normal encryption image and B_2 represents the decryption image. The NPCR and UACI results for the two datasets have been represented in Table 3 and in Table 4 respectively.

5. Case Study

This case study takes two different images, each from the MRI brain tumor data set and the COVID-19 X-Ray data set. The performance evaluation of one of the images taken from the MRI brain tumor data set is demonstrated as follows:



(a) (b) (c) (d)

Fig. 14. (a)Original image, (b) Encrypted image, (c) Attacked Image, and (d) Reconstructed (decrypted) image of MRI scan image of a brain.

Figures 15 (a-b) show the histograms of both the original image and the image that was transformed in Figure 14 (a) [41]. Figure 16. shows the comparison of encryption-decryption time of the present method with Tiny and Blowfish and Speck Algorithm. Figure 17. depicts the overlay comparison of Signcryption and Designcryption times for the proposed Ring Signature scheme with its antecedent Signature schemes like LBRS and QRS.

Table 3. Performance analysis of COVID-19 x-ray dataset

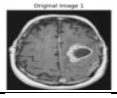
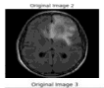
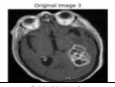
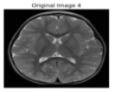
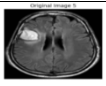
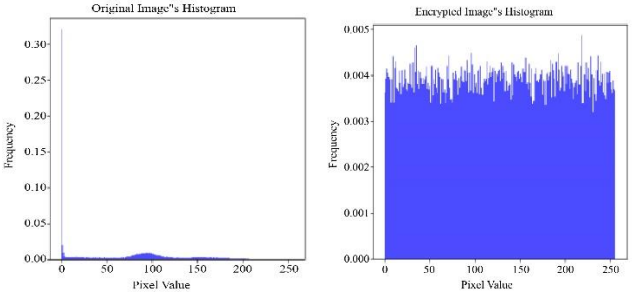
Original Image	PSNR (dB)	MSE	SSI	Entropy	MS-SSIM	NPCR	UACI
	60.30	0.06	1.000	7.72	100.00	99.65	33.53
	60.20	0.06	1.000	7.62	100.00	99.49	33.63
	60.47	0.06	1.000	7.74	100.00	99.50	33.53
	60.19	0.07	1.000	7.77	100.00	99.48	33.54
	60.55	0.07	1.000	7.84	100.00	99.90	33.61

Table 4. Performance analysis of MRI brain tumor dataset

Original Image	PSNR (dB)	MSE	SSI	Entropy	MS-SSIM	NPCR	UACI
	60.47	0.07	1.00	7.77	100.00	99.90	33.56
	60.47	0.06	1.00	7.89	100.00	99.90	33.64
	60.29	0.07	1.00	7.81	100.00	99.90	33.65
	60.39	0.07	1.00	7.81	100.00	99.91	33.60
	60.55	0.07	1.00	7.84	100.00	99.90	33.61



(a) Original image histogram **(b) Encrypted image histogram**

Fig. 15 Histograms of original image and encrypted image of MRI scan image of a brain

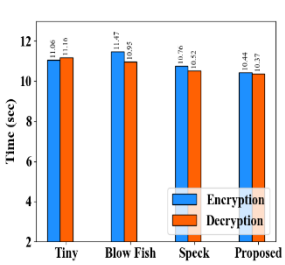


Fig. 16 Encryption and decryption time

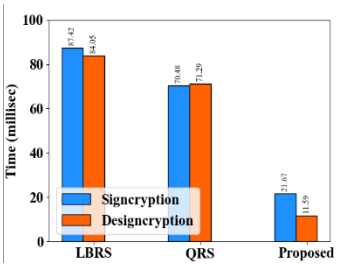
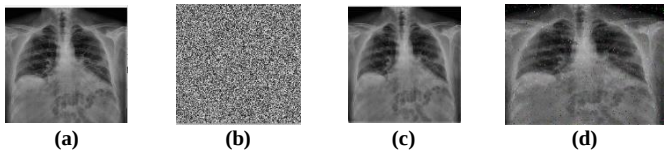


Fig. 17 Signcryption and designcryption

Listed below are the resultant correlation coefficients of the brain tumor image:

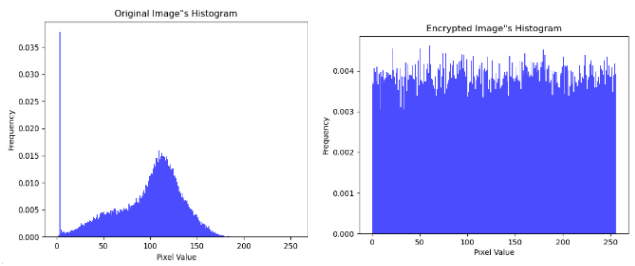
```
-----correlation co-efficients original image------

Horizontal : 0.9674628328802913
Vertical : 0.9754743338367883
Diagonal : 0.9447617459673028

------correlation co-efficients encrypted image-----

Horizontal : -0.0017527947141375442
Vertical : 0.00011297312327762478
Diagonal : 0.0011242706537876888
```

The performance evaluation of one of the images taken from the Covid-19 Chest X-ray data set is demonstrated as follows:



(a) **(b)** **(c)** **(d)**

Fig. 18 Original image, encrypted image, attacked image, reconstructed image of COVID-19 x-ray of chest



(a) Original image histogram **(b)Encrypted image histogram**

Fig. 19 Histograms of the original image and encrypted image of COVID-19 x-ray of the chest

The resultant Correlation coefficients of the original and encrypted images of the COVID-19 chest X-ray are given below:

```
-----correlation co-efficients original image------

Horizontal : 0.9762087469023265
Vertical : 0.9765155341216456
Diagonal : 0.9657291719143273

------correlation co-efficients encrypted image------

Horizontal : 0.0014986226798073543
Vertical : -0.0010729051466883094
Diagonal : -0.002635970358005305
```

The integration of SIMON encryption with the digital ring signature algorithm has resulted in a better result, when compared to the existing lightweight cryptographic algorithms- Tiny, Blowfish and Speck. This case study demonstrates better performance concerning encryption time, decryption time, signcryption, and designcryption time. The PSNR was approximately evaluated at 60 dB, while the MSE was approximated to be around 0.07, and the SSI was 1.000. A high NPCR value was estimated at 99.90, while UACI was evaluated at 33.6.

6. Comparison with Existing work

The work in this paper is related to the application of the SIMON encryption algorithm based on the configuration given in [37], integrated with the ring signature algorithm. In [37], the hardware configuration of the SIMON encryption algorithm is given. The results in this paper provide a better performance analysis when compared with the research done by the authors in Section 2.

7. Conclusion

The simulation results confirm the efficiency and success of the strategy proposed to enhance the security and efficiency of the transmission of medical data. Furthermore, the confidentiality and authenticity of the transmitted medical image are guaranteed by the proposed signcryption scheme.

Results have shown that the proposed scheme has resulted in a signcryption time of 20.28 ms for the MRI brain tumour dataset and 24.2140 ms for the COVID-19 X-ray data set, which is less when compared to the signcryption time taken by other existing methods. The SIMON algorithm also resulted in less encryption time of 10.6133 ms for the MRI brain tumour dataset and 10.4083 ms for the COVID-19 X-ray data set. The proposed scheme offers a complete secure medical image transfer solution in an IoT environment. Consequently, it has achieved improved security results. In the future, other lightweight algorithms can be applied to further improve the performance metric results.

7.1. Limitations

As the security increases by strengthening the complexity of the encryption process, the computational overhead and time complexity increase as well, which is the limitation that has been encountered in the research done in this paper.

7.2. Future Scope

In the future, other lightweight algorithms can be adapted to improve the proposed method by an IoT device for the secure transmission of medical data. Machine learning algorithms can also be used to detect and mitigate various types of attacks on data. Work is carried out based on software implementations. Further work may also include resource consumption evaluation, such as energy and power consumption, which will help to derive a complete evaluation from the perspective of both security and operational efficiency with respect to the impact that encryption has on IoT devices in healthcare.

Acknowledgment

We acknowledge the support of CVR College of Engineering for providing the infrastructure to carry out the research work.

References

[1] Mohammad Kamrul Hasan et al., "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47731-47742, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Walid El-Shafai et al., "Robust Medical Image Encryption Based on DNA-Chaos Cryptosystem for Secure Telemedicine and Healthcare Applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 9007-9035, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Maliha Sultana et al., "Towards Developing a Secure Medical Image Sharing System Based on Zero Trust Principles and Blockchain Technology," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, pp. 1-10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ray Beaulieu et al., "The SIMON and SPECK Lightweight Block Ciphers," *Proceedings of the 52nd Annual Design Automation Conference*, San Francisco California, pp. 1-6, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ronald L. Rivest, Adi Shamir, and Yael Tauman, "How to Leak a Secret," *7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast*, Australia, pp. 552-565, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ala Abdulsalam Alarood et al., "Secure Medical Image Transmission Using Deep Neural Network in e-Health Applications," *Healthcare Technology Letters*, vol. 10, no. 4, pp. 87-98, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Denghui Zhang et al., "A Privacy Protection Framework for Medical Image Security without Key Dependency Based on Visual Cryptography and Trusted Computing," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Jeeva Selvaraj et al., "Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security," *Electronics*, vol. 12, no. 7, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Tahir Sajjad Ali, and Rashid Ali, "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map," *IEEE Access*, vol. 8, pp. 71974-71992, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] M. Barbosa, and P. Farshim, "Certificateless Signcryption," *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, Tokyo Japan, pp. 369-372, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[11] John Malone-Lee, "Identity-Based Signcryption," *Cryptology ePrint Archive*, pp. 1-8, 2002. [Google Scholar] [Publisher Link]

[12] Xinyi Huang et al., "Identity-Based Ring Signcryption Schemes: Cryptographic Primitives for Preserving Privacy and Authenticity in the Ubiquitous World," *19th International Conference on Advanced Information Networking and Applications*, Taipei, Taiwan, vol. 2, pp. 649-654, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[13] Lingling Wang, Guoyin Zhang, and Chunguang Ma, "A Secure Ring Signcryption Scheme for Private and Anonymous Communication," *2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007)*, Dalian, China, pp. 107-111, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[14] Caixue Zhou, Zongmin Cui, and Guangyong Gao, "Efficient Identity-Based Generalized Ring Signcryption Scheme," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 12, pp. 5553-5571, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[15] Zheng-Hua Qi et al., "An ID-Based Ring Signcryption Scheme for Wireless Sensor Networks," *IET International Conference on Wireless Sensor Network*, Beijing, pp. 368-373, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[16] Reenu Saini, and Kunwar Singh Vaisla, "Image Signcryption Using ECC," *International Conference on Computational Intelligence and Communication Networks*, Bhopal, India, pp. 829-834, 2014. [CrossRef] [Google Scholar] [Publisher Link]
[17] Xiaodong Yang et al., "A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud," *IEEE Access*, vol. 8, pp. 170713-170731, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[18] Insaf Ullah et al., "A Lightweight and Secured Certificate-Based Proxy Signcryption (CB-PS) Scheme for E-Prescription Systems," *IEEE Access*, vol. 8, pp. 199197-199212, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[19] Ray Beaulieu et al., "The SIMON and SPECK Lightweight Block Ciphers," *Proceedings of the 52nd Annual Design Automation Conference*, San Francisco California, pp. 1-6, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[20] Pravin Mundhe et al., "Ring Signature-Based Conditional Privacy-Preserving Authentication in VANETs," *Wireless Personal Communications*, vol. 114, pp. 853-881, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[21] Lin Wang, Changgen Peng, and Weijie Tan, "Secure Ring Signature Scheme for Privacy-Preserving Blockchain," *Entropy*, vol. 25, no. 9, pp. 1-14, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[22] K. Shankar, and P. Eswaran, "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm," *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, pp. 705-714, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[23] Navoneel Chakrabarty, Brain MRI Images for Brain Tumor Detection, 2018. [Online]. Available: https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection?select=yes
[24] Covid-Chestxray-Dataset. [Online]. Available: https://github.com/ieee8023/covid-chestxray-dataset
[25] Stephanie Ang Yee Hunn, Siti Zarina Binti Md. Naziri, and Norina Binti Idris, "The Development of Tiny Encryption Algorithm (Tea) Crypto-Core for Mobile Systems," *2012 IEEE International Conference on Electronics Design, Systems and Applications*, Kuala Lumpur, Malaysia, pp. 45-49, 2012. [CrossRef] [Google Scholar] [Publisher Link]
[26] Manju Suresh, and M. Neema, "Hardware Implementation of Blowfish Algorithm for the Secure Data Transmission in Internet of Things," *Procedia Technology*, vol. 25, pp. 248-255, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[27] Lamia A. Muhalhal, and Imad S. Alshawi, "A Hybrid Modified Lightweight Algorithm for Achieving Data Integrity and Confidentiality," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, pp. 833-841, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[28] Chunhong Jiao, and Xinyin Xiang, "Anti-Quantum Lattice-Based Ring Signature Scheme and Applications in VANETs," *Entropy*, vol. 23, no. 10, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[29] Kefeng Wang, Yi Mu, and Willy Susilo, "Identity-Based Quotable Ring Signature," *Information Sciences*, vol. 321, pp. 71-89, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[30] B. Murali Krishna et al., "Security of Electronic Health Record USING Attribute Based Encryption on Cloud," *2023 4th International Conference on Electronics and Sustainable Communication Systems*, Coimbatore, India, pp. 627-632, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[31] R. Raja, and R. Saraswathi, "A Delicate Authentication Mechanism for IoT Devices with Lower Overhead Issues," *Computer Networks and Inventive Communication Technologies*, vol. 141, pp. 87-97, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[32] Fatos Xhafa, Leonard Barolli, and Flora Amato, "Advances on P2P, Parallel, Grid, Cloud and Internet Computing," *Proceedings of the 11th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Soonchunhyang University, Asan, Korea, vol. 1, 2016. [Google Scholar] [Publisher Link]
[33] Xu Han et al., "CPPA-RORS: A Conditional Privacy-Preserving Authentication Scheme Based on Revocable One-Time Ring Signature for VANETs," *Internet of Things*, vol. 27, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[34] M. Harshitha et al., "Secure Medical Data Using Symmetric Cipher Based Chaotic Logistic Mapping," *2021 7th International Conference on Advanced Computing and Communication Systems*, Coimbatore, India, pp. 476-481, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[35] Tahir Sajjad Ali, and Rashid Ali, "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map," *IEEE Access*, vol. 8, pp. 71974-71992, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[36] Lingling Wang, Guoyin Zhang, and Chunguang Ma, "A Secure Ring Signcryption Scheme for Private and Anonymous Communication," *2007 IFIP International Conference on Network and Parallel Computing Workshops*, Dalian, China, pp. 107-111, 2007. [CrossRef] [Google Scholar] [Publisher Link]
[37] Aydin Aysu, Ege Gulcan, and Patrick Schaumont, "SIMON Says: Break Area Records of Block Ciphers on FPGAs," *IEEE Embedded Systems Letters*, vol. 6, no. 2, pp. 37-40, 2014. [CrossRef] [Google Scholar] [Publisher Link]
[38] C. Shylaja, and T. Shreekanth, "Optimization of Block Cipher with SIMON," *National Conference on Power Systems and Industrial Automation*, pp. 18-23, 2015. [Google Scholar] [Publisher Link]
[39] Xiaodong Yang et al., "A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud," *IEEE Access*, vol. 8, pp. 170713-170731, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] Ming-Yang Yu, "Image Encryption Based on Improved Chaotic Sequences," *Journal of Multimedia*, vol. 8, no. 6, pp. 802-808, 2013. [Google Scholar]

[41] Salim Mushin Wadi, and Nasharuddin Zainal, "Decomposition by Binary Codes-Based Speedy Image Encryption Algorithm for Multiple Applications," *IET Image Processing*, vol. 9, no. 5, pp. 413-423, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[42] Muhammad Rizki Adiwiganda et al., "Adopting Tiny Encryption Algorithm for Patient Healthcare Record on Smart Card," *International Conference of Computer Science and Information Technology*, Medan, Indonesia, pp. 1-5, 2019. [CrossRef] [Google Scholar] [Publisher Link]