DOI: https://doi.org/10.33103/uot.ijccce.21.4.3

Image Encryption Paillier Homomorphic Cryptosystem

Zainab Mohammed Muneef[1], Hala Bahjat Abdul Wahab[2], Abdul Mohssen Jaber Abdul Hossen[3]

[1,2]Computer Science Dept., University of Technology, Baghdad, Iraq.

[3]Al-Turath University, Baghdad, Iraq

[1]cs.19.43@grad.uotechnology.edu.iq, [2]110005@uotechnology.edu.iq, [3]Abdulmohsen.jaber@turath.edu.iq

Abstract*— With the increasing use of media in communications, both academia and industry pay attention to the content security of digital images. This research presents a Homomorphic cryptosystem-based asymmetric picture encryption technique (Paillier). The algorithm is used for securing images that transmit over public unsecured channels. The Homomorphic property is used in this paper, which is comprised of three steps: key generation, encryption, and decryption. To realize such approach, the encryption cryptosystem must support additional operation over encrypted data. This cryptosystem can be effective in protecting images and supporting the construction of programs that can process encrypted input and produce encrypted output.*

Index Terms *—Homomorphic, Partiall HE, Paillier Homomorphic, Encryption.*

I. INTRODUCTION

Most companies now outsource data storage in a reliable and secure manner due to the widespread use of electronic data, necessitating the development of techniques to ensure this [1]-[3]. External data centers provide storage space and allow organizations to encrypt and securely store confidential data. As a result, the secret key can only be used by the registered owner of the secret data to access the stored data. Recently, there has been a demand for statistical and mathematical computations, as well as predictive analysis, on encrypted data. However, since encrypted data must be decrypted as original data for such processing, traditional data centers lack the necessary computing techniques. Data is highly vulnerable at this stage, and searching and decrypting the data would increase the computation time [4]-[5].

The encryption technology means that the procedures on the encrypted data and matching result can be attained as on original data, according to Homomorphic Encryption (HE). The cipher text can be subjected to mathematical operations without changing the encryption's essence. With HE, a company can encrypt its database and upload it to the cloud, and the data can be processed without having to decrypt it; in other words, Homomorphic encryption cryptosystems perform operations on encrypted data without requiring the client's private key [6]-[7]. The RSA and ElGamal cryptosystems describe two different types of asymmetric cryptosystems. Pascal Paillier suggested an additional class of asymmetric cryptosystems in 1999. Paillier is a public key cryptosystem with additive homomorphism, which makes it appropriate for privacy-sensitive applications [8]. This paper focuses on Paillier's early work in homomorphic encryption by demonstrating how to encrypt and decrypt images using this cryptosystem, as well as the underlying mathematical ideas that make the system works clearly and obtaining secure encryption.

Received 20/5/2021; Accepted 17l10l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.4.3

The literature reviews of some of the published papers have been done, which is briefly described below:

In [9], Radjab Harerimana et al. showed how to implement the Paillier Homomorphic Encryption (HE) technique by using the Java API. The Pailler HE library was used in an electronic voting system which is a proof of the main concept, allowing and letting the voting server to aggregate candidate votes in an encrypted form while keeping voters unknown.

In [10], Taiwo Blessing Ogunseyi and Tang, with the changed in storage paradigm, a greater demand nowadays for the dataset privacy as well as the encryption scheme that allows the computations on encrypted data. As an example of a Homomorphic encryption scheme is Paillier cryptosystem. They proposed an improved decryption method to enhance the performance of Paillier Homomorphic encryption scheme in terms of the decryption speed and the overall cost of computations. In particular, the use of the variable k to simplify multiplicative modular arithmetic. These Experiments showed that the method is very efficient in terms of decryption peed.

In [8], Tanyaporn Sridokmai and Somchai Prakancharoen, one of Paillier's encryption schemes, as well as Homomorphic encryption, was demonstrated in this article. Subtraction, Multiplication, and Division binary operations of binary dependent integer number operands were presented in mathematical detail. The confidentiality of encryption and decryption will be shown in particular. Even though another operation was in progress, both operands remained encrypted.

In [6], Majedah Alkharji and Hang Liu, the proposed model successfully analyzed image processing and was able to use homomorphic encryption techniques in order to create a safe and reliable communication channel. Consistent data security measures.

II. HOMOMORPHIC ENCRYPTION (HE)

Homomorphic encryption is a new topic of security which many researchers focus on, because it provides higher security for the data, especially in the cloud computing environment, the client is the only key owner in the homomorphic encryption scheme, allowing operations on encrypted data without even knowing what is the private key (no need to decrypt). The decrypt of results for any kind of operation, which is equivalent to the calculation, is carried out on the raw data. HE techniques are partial, somewhat and fully homomorphic encryption. The purpose is to store, transmit and process ciphertext safely to maintain data integrity and confidentiality [11].

In today's always-on, Internet-centric world, data privacy is more critical than ever. Numerous cryptographic techniques have already been developed to improve data protection throughout the communication and storage processes. These techniques have been employed, but they are virtually useless because they demand that the data be visible to the cloud provider. To accomplish this, the private key must be provided to the server, which will complete the necessary actions. This issue has been resolved by the use of privacy homomorphism. Homomorphic encryption enables us to perform mathematical operations directly on the ciphertext while maintaining the secret key required to decrypt the output. Along with preserving in terms of privacy, it produces the same result as if the computations were performed in plaintext. Therefore, used the homomorphic paillier algorithm in this paper.

A. Properties of the Homomorphic Encryption

The Homomorphic systems can be defined in line with the operation that allows to perform on the original data as following [6]. Additive homomorphic encryption (for

Received 20/5/2021; Accepted 17l10l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.4.3

example, G and paillier cryptosystem) or multiplicative homomorphic encryption (for example, RSA and El-Gamal cryptography).

HE allows Server execution complex mathematical calculations on encrypted data without having to acknowledge the original data. In more details, given a plaintexts m1⨁ m2, and the corresponding cipher texts c1 ⨁ c2, a HE scheme allows the processing of c1 Θ c2 leaving out the applying of pk1 Θ pk2, Where c is cipher, pk is public key.

In that connection, the cryptosystem is either additive or multiplicative Homomorphic in nature depends on the Θ operation, which can be either addition or multiplication [12].

- The Additive Homomorphic Encryption (AHE): The additive operation allows the HE schemes to evaluate raw data. The following scholars who are Paillier, GM and Benaloh, and Okamoto-Uchiyama made cryptosystems that are examples of this method. Scholars assert that HE is additive if: E (m1⨁m2) =E (m1) ⨁ Em2), without even knowing (m1), and (m2) [13].
- The Multiplicative Homomorphic Encryption (MHE): A homomorphic multiplicative scheme is a phrase used to describe a scheme that is both homomorphic and multiplicative. The term property refers to systems that create cipher texts from a collection of plain texts. The Elgamal and RSA cryptosystems are multiplicative homomorphic methods. we can consider the Homomorphic encryption as a multiplicative method if only: E (m1⨂ m2) = E (m1) ⨂ E (m2), without even knowing what (m1), and (m2) are [14].

III. PARTIALLY HOMOMORPHIC ENCRYPTION (PHE)

In partly homomorphic encryption, the ciphertext can be subjected to one of two operations: addition (ex: paillier and GM cryptosystem) or multiplication (ex: RSA and El-Gamal cryptosystem), but not both [6].

A. Paillier Homomorphic Encryption

The Paillier cryptosystem is a probabilistic public key cryptosystem. It is a highly effective additively Homomorphic encryption scheme [10]. Because of its nondeterministic existence, The Paillier cryptosystem is widely utilized in applications such as privacy-preserving safe computation, secure electronic voting, electronic financial transactions, and other applications. This scheme is based on the decisional composite residuality assumption in mathematics [8]. The scheme has three algorithms described as follows:

—Key Gen Algorithm: Calculate n = p q and λ = LCM (p − 1, q − 1) LCM means Least Common Multiple, for large primes p and q such that gcd (p q, (p − 1) (q − 1)) = 1. Then, instead of n as in the Benaloh cryptosystem, verify whether gcd (n, L (gλ mod n^2)) =1, where the function L is defined as L (u) = (u − 1)/n for any u from the subgroup Z× n^2, which is a multiplicative subgroup of integers modulo n^2. Finally, the secret key is a (p, q) pair, while the public key is (n, g) [4].

— The Encryption Algorithm:

The number r is selected at random for each message m, and the encryption works as follows [8]:

$$C = E(m) = g^m r^n (\text{mod } n^2) \tag{1}$$

—The Decryption Algorithm: For a proper cipher text c < n2, the decryption is done by [10].

Received 20/5/2021; Accepted 17l10l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.4.3

$$D(c) = \frac{L\,(c^{\lambda}\,(mod\;n^2)}{L\,(c^{\lambda}\,(mod\;n^2)}\;\; Mod\; n \;=\; m \qquad (2)$$

Where the private key pair is (p, q).

— The Property of Homomorphic [8]:

$$\mathrm{E(m1)} \times \mathrm{E(M2)} = \left(\mathrm{g^{m1} r_1^n\ (mod\ n^2)}\right) \times \left(\mathrm{g^{m1} r_2^n\ (mod\ n^2)}\right)$$

$$= \mathrm{g^{m1+m2}\,(r_1 \times r_2)^n\ (mod\ n^2) = E(m_1 + m_2)} \qquad (3)$$

Paillier encryption scheme is Homomorphic over addition, as seen by this derivation. Additional Homomorphic features that exist in Palliser are an encryption technique, which allow extra basic operations on original image m1, m2 ∈ Z×n2 By using the encrypted plaintexts E (m1) and E (m2) and public key pair (n, g) [2],[12]:

$$\mathrm{E(m1) \times E(M2)(mod\ n^2) = \ E(m_1 + m_2)(mod\ n),} \qquad (4)$$

$$\mathrm{E(m1) \times \left(g^{m2}\ (mod\ n^2)\right) = \ E(m_1 + m_2)\ modn\,,} \qquad (5)$$

$$\mathrm{E(m1)^{m2}\ (mod\ n^2) = (m1m2(mod\ n)} \qquad (6)$$

These additional homomorphic characteristics describe numerous cross-relationships between encrypted and plaintext processes. Equations (4), (5) and (6) in other words, show how actions performed on encrypted data influence the original image.

IV. THE PROPOSED FRAMEWORK

We propose a Paillier algorithm based on the advantages of homomorphic encryption in providing efficient security for original data for image encryption and decryption. The partial Homomorphic property is satisfied by the proposed algorithm. It supports additive homomorphism. Because of its nondeterministic nature, Paillier cryptosystem is usually used for privacy-preserving safe secure electronic voting, computations, and financial transactions using electronics, among other applications. The proposed structure is depicted in Fig. 1.

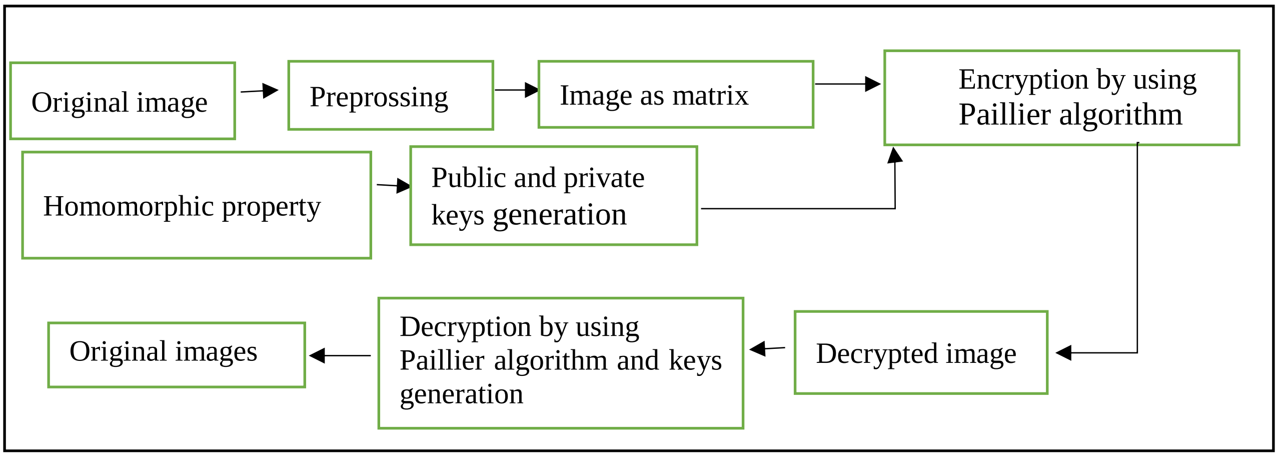
Original image
Prepressing
Image as matrix
Encryption by using Paillier algorithm
Homomorphic property
Public and private keys generation
Original images
Decryption by using Paillier algorithm and keys generation
Decrypted image

FIG. 1. ARCHITECTURE PROPOSED FRAMEWORK.

Some of the steps of the proposed system are given below:

1. Original images are taken, this image is color (R, G, B).
2. Prepressing for image (Resize).
3. The image is turned into a matrix 2D in order to run the encryption operation on this data, where the data is encrypted for each pixel in the image.
4. One by one, these matrix members are sent to the suggested formula.

Received 20/5/2021; Accepted 17l10l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.4.3

5. Two keys were generated, public and privet. The public key is used to encrypt images. The private key is used to decrypt images.
6. The public and private keys are produced using the Homomorphic property.
7. Encrypt data by using public key for paillier algorithm and encrypt equation.
8. The encoded matrix is transformed into an image.
9. The encrypted image can then be stored.
10. The decrypted matrix is then transformed into an image.
11. The original image is obtained.
12. The researchers will use these encrypted files.

The proposed system uses Partial Homomorphic Characteristics to encrypt sets of images with different content and sizes. The results were measured using PQE measures, histogram, and entropy. It was found that the paillier algorithm used gives secure encryption, but in terms of time, we noticed through the implementation of the program that the paillier takes a long time to encrypt and decrypt.

V. RESULTS

The followings are the results of the proposed cryptographic model (image encryption by using partial Homomorphic). In terms of the image cryptosystem shown in Fig. 1, It was used the plain images Lena 256×256, Paper 256×256, Baboon 560×560, Barbra 512×512, and all are color images and the test results are shown in Fig. 2.

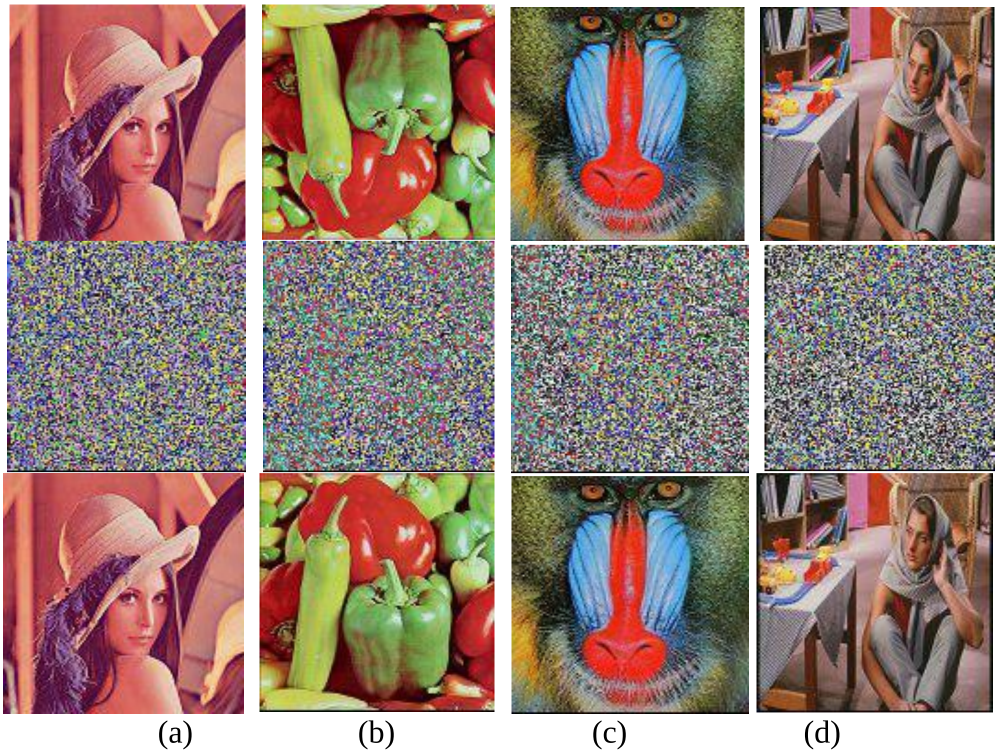

FIG. 2. RESULTS OF THE PROPOSED CRYPTOGRAPHIC. (A) LENA (B) PEPPER (C) BABOON (D) BARBRA

In the proposed method, we used a different quality and sizes image tests for the evaluation of the efficiency and the security of the proposed system. By using Picture Quality Evaluation (PQE), Histogram Analysis, tests randomness and the Evaluation of Image Quality by an Entropy. One of the disadvantages of this work is that it is slow.

Received 20/5/2021; Accepted 17l10l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.4.3

A. Experimental Results Test

We can deduce the following from the results of the measures used to test the ciphered images, which are provided in Table 1: -

1. The large MSE findings (as seen in the tables below) indicate that the suggested approach was successful in hiding pure image information.

2. The low SNR and PSNR values indicate that the proposed Homomorphic algorithm generated a lot of noise (i.e., a low result implies better image encrypt of the original image).

3. The AD shows the main difference between the plain not encrypted images and the cipher images, it is divided by MSE. The MD shows the maximum error result between the plain and the cipher images. The both images must be changed and converted to grayscale images with a range of 0 to 255, and NC must be shown in all images equal 1. Because it is indicating disparities between the plain image and the cipher image. Between the plain image and the decrypted image must be a large number. MAE follows the same concept. MSE instead of doing the square difference between the plain and decrypted images calculated absolute, Normalized Absolute Error (NAE) differences are determined by the sum of the pixel quadratic value between the initial and decoded picture, must show 1 if there is no deformation happened between the plain and the decrypted images, but the result evaluation showed less than one**.** Where Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Average Difference (AD), and Maximum Difference (MD), Normalized Cross correlation (NC), Mean Absolute Error (MAE), Normalized Absolute Error (NAE), Structural Content (SC), Signal-To-Noise Ratio (SNR), and Similarity Measure (SIM).

TABLE 1. (PQE) MEASUREMENTS.

Name	MSE	PSNR	AD	MD	NC	MAE	NAE	SC	SNR	SIM	UACI
Lena	9119.9	0.005	3864	231	0.216	1.026	0.216	7729.5	2.14	129.7	34.09
Pepper	10103.2	0.004	4199.5	227	0.236	1.235	0.236	8399.0	2.05	123.7	35.62
Baboon	10103.2	0.005	4199.5	229	0.236	1.235	0.236	8399.0	2.057	123.7	35.62
Barbra	10103.2	0.004	4198.5	228	0.236	1.235	0.236	8399.0	2.057	123.7	35.62

B. Histogram analysis

The histogram of an image means graphing the number of pixels inside the image to show how the pixels are distributed in the whole image. For a plain picture, a good image encryption method must always produce a cipher image with a histogram which uniform. histograms of a few encrypted images, as well as the original images with widely disparate material, were measured and analyzed. Fig. 3 gives the histograms for the famous Lena photogram, Paper, Baboon and Barbra images, respectively. We evaluated and found out the following Fig. 3 (a, b, c, d) that the regular and plain image histograms are not precise and accurate, whereas the encrypted digital image histograms have been reliable and more precise.

Received 20/5/2021; Accepted 17l10l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.4.3

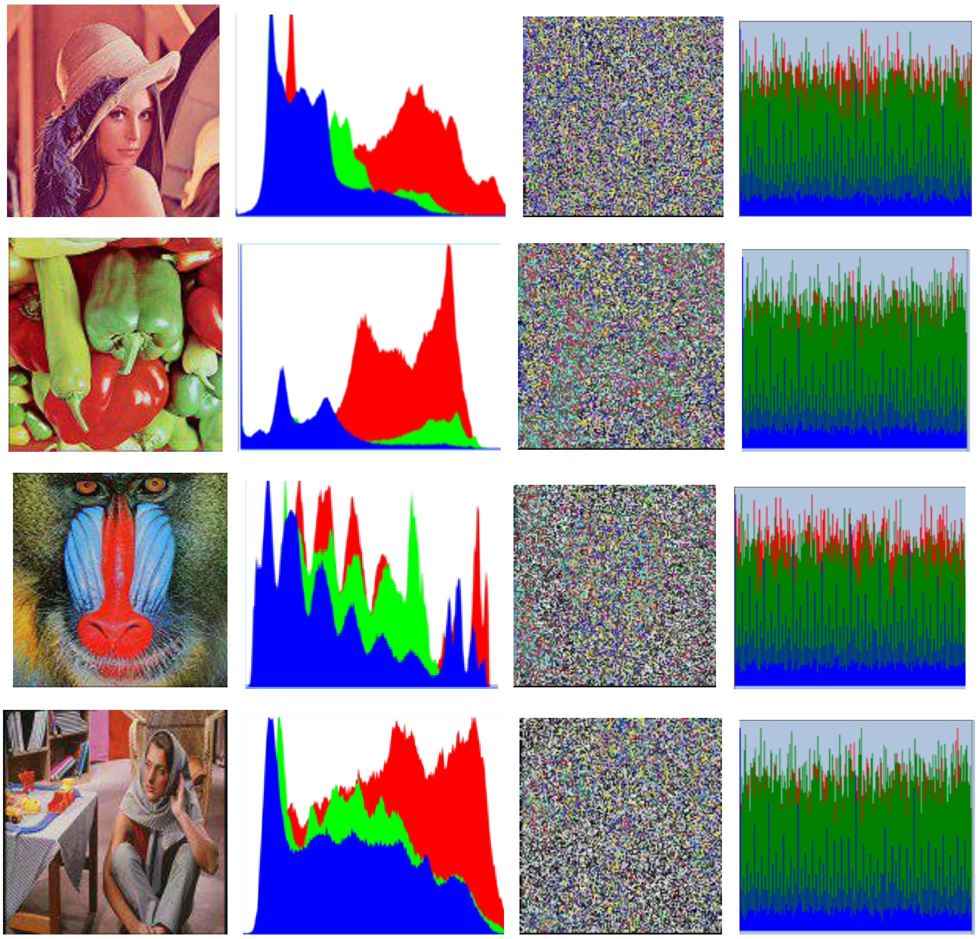

FIG. 3. HISTOGRAM ANALYSIS. (A) LENA (B) PEPPER (C) BABOON (D) BARBRA

C. *Information entropy analysis*

In information theory, an entropy is a statistical measure of the randomness. The entropy H (s) is calculated and found out by using Eq. (7). $p(s_i)$ is the likelihood of the symbol mi and the entropy is found out and must be measured in bits [5]. The cipher image pixels values must be very random. The entropy value of any good cipher image must be about 8. The different entropy values of the previous encrypted image are shown in Table 2.

$$H(s) = -\sum_{i=0}^{2n-1} p(s_i) \log_2 p(s_i) \quad (7)$$

TABLE 2. ENTROPY VALUES OF THE CIPHER IMAGE

Name	Lena	Pepper	Baboon	Barbra
H (s)	7.8919	7.888	7.8887	7.8887

.

Received 20/5/2021; Accepted 17l10l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.4.3

VI. CONCLUSION

Homomorphic Encryption has remained a significant research area until recently. In this work, the Paillier encryption algorithm was used to encrypt and decrypt images. The public and private keys were developed based on the Homomorphic property to optimize the efficiency of encrypting images and provide high security for images while they are stored. One of the disadvantages of this work is that it is slow. In the future, we propose using elliptic curves with Homomorphic, to improve the speed of the algorithm used.

REFERENCES

[1] A. S. Hamad and A. K. Farhan, “Image Encryption Algorithm Based on Substitution Principle and Shuffling Scheme,” Eng. Technol. J., vol. 38, no. 3B, pp. 98–103, 2020, doi: 10.30684/etj.v38i3b.433.

[2] A. M. Rahma, A. M. Hossen, and O. Dawood, “Public Key Cipher with Signature Based on Diffie-Hellman and the Magic Square Problem,” Engineering and Technology Journal, vol. 34, no. 1, pp. 1–15, 2016.

[3] N. A. Hassan and A. K. Farhan, “Security Improve in ZigBee Protocol Based on RSA Public Algorithm in WSN,” Eng. Technol. J., vol. 37, no. 3 B, pp. 67–73, 2019.

[4] B. Rani, "A novice’s perception of partial homomorphic encryption schemes." Indian Journal of Science and Technology, vol. 9, no. 37, pp.10--18, 2016.

[5] N. Sushmetha, S. Vairamuthu and B. Rani, "A Case Study on Partial Homomorphic Encryption : Breast Cancer Diagnosis," International Journal of Pure and Applied Mathematics, vol. 119, no. 7, pp. 155–9, 2018.

[6] M. Alkharji, H. Liu, and C. U. A. Washington, "Homomorphic encryption algorithms and schemes for secure computations in the cloud." In Proceedings of 2016 International Conference on Secure Computing and Technology, pp.19, 2016.

[7] Z .Hikmat and M. K. Ibrahem, "Homomorphic Encryption Security for Cloud Computing systems," Al-Nahrain University, vol.19, no.1, pp. 1-4, 2020.

[8] T. Sridokmai, and S. Prakancharoen, "The homomorphic other property of Paillier cryptosystem." In 2015 International Conference on Science and Technology (TICST). IEEE, pp. 356-359, 2015.

[9] R. Harerimana, S. Y.Tan, and W. C. Yau, "A Java implementation of paillier homomorphic encryption scheme." 2017 5th International Conference on Information and Communication Technology (ICoIC7). IEEE, pp.1-6, 2017.

[10] T.B. Ogunseyi, and T. Bo, "Fast decryption algorithm for paillier homomorphic cryptosystem." 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS). IEEE, pp. 803-806, 2020.

[11] R. F. Hassan, and A. M. Sagheer, "A Proposed Secure Cloud Environment Based on Homomorphic Encryption" Iarjset, vol. 6, no. 5, pp. 166–75, 2019.

[12] I. F. Elashry, O. S. F. Allah, A. M. Abbas, S. El-Rabaie, and F. E. Abd El-Samie, "Homomorphic image encryption." Journal of Electronic Imaging, vol. 18, no. 13, pp. 033002, 2009.

[13] A. Acar, H. Aksu, A. S.Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation." ACM Computing Surveys (CSUR), vol. 51, no.4, pp. 1-35, 2018.

[14] D. K. Rappe, "Homomorphic cryptosystems and their applications." Cryptology ePrint Archive, 2006.

[15] L. Li, A.A. Abd El-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images." Signal Processing, vol. 92, no. 4, pp. 1069-1078, 2012.

Received 20/5/2021; Accepted 17l10l2021