Journal of Theoretical and Applied Information Technology
15th October 2018. Vol.96. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HYBRID HOMOMORPHIC CRYPTOSYSTEM FOR SECURE TRANSFER OF COLOR IMAGE ON PUBLIC CLOUD

[1]HAIDER M. AL-MASHADI, [2]ALA'A A. KHALAF

[1] Information System Dept., College of Information Technology, University of Basra, Basra, Iraq

[2] Computer Science Dept., College of Science, University of Basra, Basra, Iraq

E-mail: [1]mashhad01@gmail.com , [2]alaa.almakhzomy@yahoo.com

ABSTRACT

Cloud computing is a model of advanced computing that has an important impact on information technology and provides access to the shared digital resources that existed in cloud servers by using Web services. Great benefits for users through cloud computing such as social networking, banking, finance, storage, e-mail, and many features related to flexibility, ease of use and reliability with high performance and low cost. On the other hand, cloud applications and information are vulnerable to security breaches by unauthorized parties as a result of the shared and online resource environment, which requires protection through appropriate policies, techniques and controls to protect published data, applications, infrastructure and related components of cloud computing. This paper presents three efficient hybrid homomorphic encryption techniques for image encryption to ensure the safe exchange of private images in the public cloud based on the block pixel position. The proposed techniques are constraint on El-Gamal and Enhanced Homomorphic Cryptosystem (EHC). Many methods of security analysis have been implemented on proposed techniques which used many types of images with many experiments. The results showed that our methods are very invulnerability and efficient in terms of security and time compared with El-Gamal and EHC schemes, because they take the good characteristics of El-Gamal and EHC methods like very good security and small run time executions.

Keywords: *Cloud Computing; El-Gamal cryptosystem; Homomorphic Encryption Cryptosystem; Enhanced Homomorphic Cryptosystem; Cryptography.*

1. INTRODUCTION

NIST describes cloud computing as "a model for enabling appropriate and demand-driven access to a network of configurable computing resources (e.g. servers, networks, applications, services, and storage) that can be quickly delivered and released with minimal administrative effort or interaction". NIST defines four publishing models: public, private, community, and hybrid cloud [1]. This paper focuses on public cloud, which is a cloud infrastructure that serves the general public or wide range of organizations [2]. Public cloud services may be free or rather inexpensive. The public cloud does not mean that user data is generally visible; cloud vendors generally provide an access control mechanism for users, such as Google and Amazon, which serve businesses and consumers online [3].

However, the public clouds are the least safe model compared to other cloud models so that all data and applications on public cloud are more prone to malicious attacks [4]. Cloud computing is used to store a large amount of data which allows consumers to access these data remotely from anywhere and at any time in the future instead of storing data in hard drives such as hard disc, pen drives and CD-ROMs. As the data owners tend to store their data in a cloud which is the latest trend of storage technologies [5]. Information security is very useful in our daily lives and this is very important and digital images are one of the data that users usually need to ensure their security. Reliable image encryption techniques are great importance to protect data from fraud, tampering and unauthorized access [6]. This paper try to enhance the security of transferred images on the cloud by implementing three hybrid scenarios on tow

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

encryption algorithms El-Gamal and Enhanced Homomorphic Cryptosystem (EHC) to produce the proposed three hybrid cryptosystems.

2. LITERATURE SURVEY

A. Edi et al. [7] used partial homomorphic encryption based on the El-Gamal scheme to achieve image security. Authors explained how to multiply many of cipher images to be more resisted to cracking. They use the statistical test MSE (Mean Squared Error) to check errors detection by comparing the original image and decrypted image. Results of testing MSE were 0 this illustrates that the original image decrypted image is exactly identical.

X. Zhang et al. [8] apply a new technique of scalable coding for cipher images. The pseudorandom numbers which are derived from a private key are masked by a modulo-256 and added with original pixels of the image. And then, quantize the encrypted image with Hadamard coefficients.

C. Song et al. [9] used a chaotic cryptosystem for image encryption which provides low computation complexity. The encryption process is implemented in the client equipment. Finally, compress the encrypted image by a new lossy compression technique which it is based on the compressive sensing CS.

B. Pan et al. [10] they propose an encryption scheme based on RSA, AES, and Murmur-Hash. In the proposed method, the pixels are encrypted with RSA and AES separately, and to achieve image integrity, Murmur-Hash is embedded in the encrypted image, thus improving both security and performance. The encrypted image is decrypted without any loss of information.

A. Bilakanti [11] proposed fully homomorphic cryptosystem based on the learning with errors (LWE) problem, which is a modified scheme of the BVG cryptosystem for image encryption that provides fewer computations over the cloud. This scheme modifies basic LWE based on fully homomorphic encryption to process decimal inputs directly as like in BGV cryptosystem.

Y. Li et al. [12] proposed a new technique to reduce the expansion of ciphertext in image encryption based on homomorphic cryptosystem. The strategy of the proposed method based on the random selection of image pixel subset and encrypts the selected subset using homomorphic encryption while the other pixel's subsets are encrypted using linear interpolation by relating them with the random subset. This proposed approach is secure and achieve the expansion of the cipher text problem while still preserving the homomorphic property.

S. Chandel and Patel [13] use the RSA algorithm for encrypts the images encryption to achieve the image security in the communication. The selected image file is split. The split image encrypted by the RSA algorithm and then combines the encrypted split image and produces an encrypted image in decryption process on the encrypted image in the same way. To evaluate the security of the proposed approach, Histogram and entropy are used. The experimental results illustrate the effectiveness of the proposed method.

H. Saleh et al. [14] propose a secure and effective searching system over encrypted images in private cloud and design a new asymmetric encryption algorithm by combining RSA and Paillier schemes. The proposed encryption method achieved higher security with good processing time. The proposed method evaluated by PSNR, Entropy, NPCR, UACI and processing time.

3. SECURITY IN PUBLIC CLOUD

Despite increased data breaches and hacking in the public cloud, data security can be achieved with high-quality security solutions based on the use cryptograph [15]. Cryptography is the science that deals with information security and protection against unauthorized access. It is achieved by converting this sensitive information into a form incomprehensible by attackers though stored and transmitted.

The main purpose of cryptography is to keep the data in secure from unauthorized users. Data encryption mostly is a scramble for data content, such as text, image, audio, and video to compose unreadable, intangible or incomprehensible data during communication or storage. The reverse of data encryption process is called data decryption. Because of the security features of cryptography it is used on a wide scale today, cryptography provides a number of security objectives such as: [16]

1) Authentication: is intended to verify user identity. Identity and authentication management is concerned with preventing unauthorized persons from accessing IT resources [17].

2) Confidentiality: means that protected data is only accessed by authorized persons who have permission access to the protected data. [18].
3) Data Integrity: refers to the protection of data from modification, deletion, theft or unauthorized fabrication. User data rights are protected by preventing unauthorized persons from unauthorized access to data, manipulation, misuse or theft of data [19].
4) Non-Repudiation: A process to prove that the sender sent this message. In other words, the sender is not allowed to deny his message.
5) Access Control: means that only authorized parties are able to access the given information.

4. HOMOMORPHIC ENCRYPTION CRYPTOSYSTEM

Security of communications and data is paramount important as digital communication and networks are constantly growing and evolving. Communication security is achieved by using encryption with aim of ensuring the confidentiality of data in communications and storage. The problem of encryption occurs when you are required to publicly compute private data or to modify a function or algorithm somehow make sure that it is still executable with privacy guarantee [20]. This can be achieved by using an encryption system which is homomorphic encryption techniques. This technique has significant advances in computing, particularly in cloud computing. Homomorphic encryption provides a way to securely transfer and store confidential information across and in a computer system [21]. The essential property of homomorphic cryptosystems is that the computation that performed on the encrypted data gives the same result if implemented on plain data. [22]. Homomorphic cryptosystem includes four basic functions: key generation, encryption, decryption, and evaluation process. In Evaluation process, the operations are performed on the encrypted data without using private key. When we decrypt the result of evaluation algorithm, it gives the same result as if we performed the operation on the original data [23]. Homomorphic cryptosystems are classified to three models according to the operations that performed on the data [24]:

1) Partially Homomorphic Cryptosystem: Allows one operation to be performed on encrypted data such as addition or multiplication.
2) Somewhat Homomorphic Cryptosystem: Has various operations which are allowed to be performed on encrypted data, with a limited range of multiplication and addition operations.
3) Fully Homomorphic Cryptosystem: Supports unlimited number of mathematical operations to be performed on encrypted data from the previous two models.

5. EL-GAMAL ENCRYPTION SCHEME

In 1985, Tahir El-Gamal has been developed El-Gamal scheme which bases on discrete logarithm problem for finite fields. Algorithm (1) explains the steps of El-Gamal Cryptosystem [25]:

Algorithm (1). El-Gamal cryptosystem

Key generation
• Choose a large prime number p • Choose the base alpha $< p$. • Choose the private key $a < p$. • Compute beta = alpha ^{a}(mod p)
Public keys:{ p, alpha and beta } private key:{a}
Encryption of a message
Input : Massage m
• Choose a secret random number $k \in [2 –, p-2]$ • Compute c_1= alpha ^{k}(mod p) • Compute c_2= beta ^{k} (mod p) × m
Output: c= {c_1,c_2}
Decryption of a message
• Compute m= $c_1^{-a} \times c_2$ mod p • Output : original massage m

El-Gamal is efficient algorithm for security according to use discreet numbers that make crashing the key is more difficult. However, this algorithm is time consuming because it use complex operation in encryption and decryption but it a strong method duo to the randomization of encryption process that led to make the cipher text for a specific message m is not repeated. However; the randomization can protects the cipher text from attacks such as a probable text attack. Additionally, because of the robust structure of El-Gamal

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cryptosystem, there is no relation between the encryption of message1, message2 and message1*message2, or any other simple operation of message1, and message2 which other systems lack for this feature such as RSA cryptosystem [26]. In other hand, El-Gamal cryptosystem need for randomness that makes it slow especially when used for digital signature. The other drawback of the El-Gamal cryptosystem is that message is encrypt to (c1, c2) which means the cipher text is twice as long as the plaintext [27].

6. GORTI'S ENHANCED HOMOMORPHIC CRYPTOSYSTEM (EHC)

Nowadays, holomorphic cryptosystem have been frequently used in different applications. In 2013, Gorti & et al. proposed EHC which is the new Enhanced Homomorphic Cryptosystem. The steps of EHC are explained in the algorithm (2) below [28].

Algorithm (2) EHC cryptosystem

KEY GENERATION
• Choose a large prime number p and q ($p > q$) • Compute $n = p \times q$
public key: {n} private key: {p, q}
Encryption of a message
• Input : Massage m • Generate a random number r • Compute c = $m + r \times p^{q} \bmod n$ • Output: c
Decryption of a message
• Compute m= c mod p • Output : original massage m

EHC can be describe as follow: [29]

1) At encryption steps, the algorithm uses the private keys q, and p and r. the keys are too large so it takes long time to hack these private keys.
2) The private key will randomly be generated for each encryption process. This leads to the fact that the same plain text does not give the same cipher text, this prevents the intruder from breaking the cipher text even if has a strong observation.
3) EHC is a fully homomorphic cryptosystem which support both addition and multiplication.
4) Decryption takes a short time.
5) In terms of performance, EHC consumes less memory and power.

7. PROPOSED METHOD

This part of the study is concerned with how to preserve the secure exchange of images in public cloud environment, where it was explained earlier, that public cloud is the most common models of the cloud vulnerable to threats and security breaches. Figure1, illustrate the proposed method mechanism.

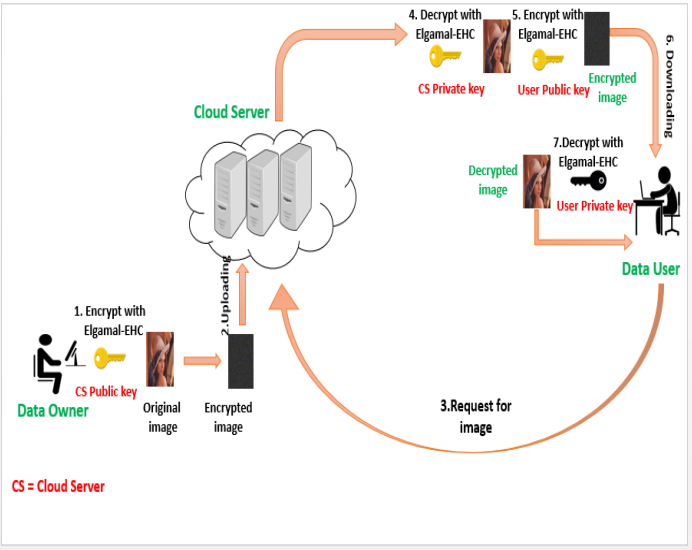

Figure 1: Proposed method mechanism

Figure 1, illustrate Three essential entities which are the basic components of the system are Data Owner, Cloud Server Provider, and Data User. Two basic processes are performing:

1. **Image Uploading:** Data owner will encrypt the demand image by hybrid homomorphic cryptosystem El-Gamal-EHC and the public key of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cloud server provider. After that, upload the encrypted image to store it in the cloud server.

2. **Image Downloading:** When data user request for a specific encrypted image, the cloud server will decrypt the demanded image with cloud server's private key and encrypt the image again with user public key of data user. The cloud server sends the encrypted image to the data user. The data user will decrypt image with his private key.

The main objective of this process is to preserve image data from unauthorized access by using hybrid cryptosystem which applied to encrypt the images using El-Gamal-EHC in order to achieve its security and prevent unauthorized members from accessing when images are exchanged on the public cloud.

This operation will keep the encrypted image from alteration and breaching caused by attackers and intruders such as a man in the middle attack. In this research, This paper l illustrates three techniques of hybrid homomorphic cryptosystem based on exploit the spatial block pixel position, these techniques are:

- El-Gamal-EHC based on Odd and Even block index (EEOE). the algorithm of this method shown in Figure 2.
- El-Gamal-EHC based on block position in lower Triangle (EEBPT), the algorithm of this method shown in Figure 3.
- El-Gamal-EHC based on Zigzag Scan and Counter (EEZSC), the algorithm of this method shown in Figure . 5.

In order to achieve the security and prevent unauthorized members from accessing when images are exchange on the public cloud, the hybrid cryptosystems are applied to encrypt the images using El-Gamal, on the other hand using EHC for reduce the execution time and expand the strength of cryptosystem.

In order to encrypt color images, they go through several stages as shown in Figure 2:

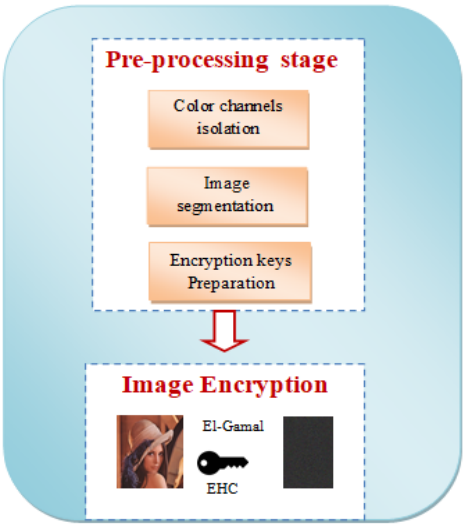

Figure 2: Image Encryption Stages

A. Pre-processing stage:

1. In preprocessing stage, the original image which it is 256 ×256 pixels is separated into its three color layers: Red, Green and Blue layer.

2.Each layer is segmented into 32× 32 blocks that result in 1024 blocks for each layer which every block is 8×8 pixels. The resulted segmented blocks are stored into an array which is in EEOE is a one-dimensional array and other schemes (EEBPT and EEZSC) is a two-dimensional array.

3.Key preparation: in this stage, the private and public keys are generated. In all the images encryption models presented in this study, a homomorphic hybrid system is used that combines El-Gamal and EHC schemes. Both schemes are asymmetric or so-called public key algorithms which use two different encryption and decryption keys. The plain image is encrypting with the public key and decrypting with the private key.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

B. Image Encryption:

In the encryption phase, the block-based encryption is used as the hybrid use of the El-Gamal and EHC algorithm based on the spatial positions of blocks. Three encryption schemes are proposed which described in the following subsections.

1. El-Gamal-EHC based on Odd and Even block index (EEOE)

In the encryption process of EEOE scheme, the segmented blocks which are stored in 1D-array, the blocks that are in the odd index of the array are encrypted with EHC and the blocks which are in the even index are encrypted with El-Gamal.

In decryption process, the same way is followed, the blocks that are in the odd index of the array are decrypted with EHC and the blocks which are in the even index are decrypted with El-Gamal.

In this structure, there is a fair distribution between using both of algorithms, where 512 blocks are encrypted with El-Gamal and 512 with EHC. This achieves high security and difficulty of hacking due to the general characteristics of the two algorithms, but it will be slower because of the El-Gamal algorithm is slower than EHC. Figure 3 illustrate the basic steps of EEOE scheme.

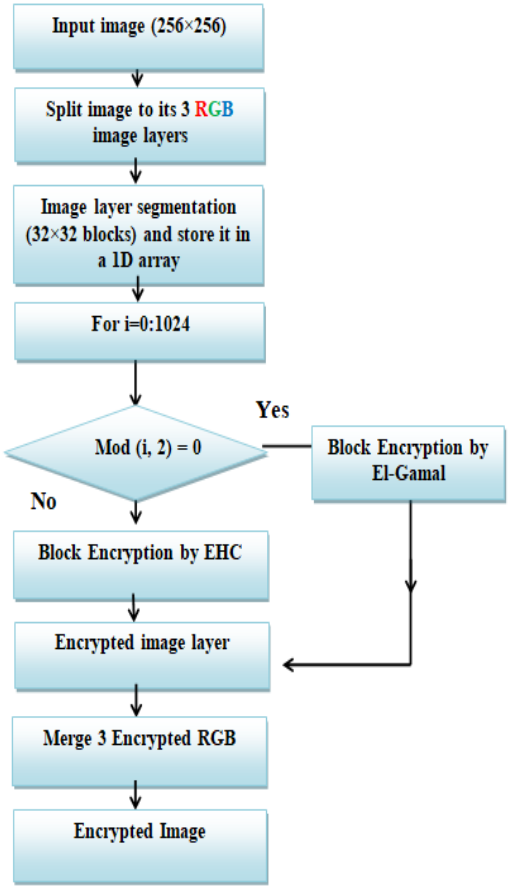

Figure 3: El-Gamal-EHC based on Odd and Even block index (EEOE)

2. El-Gamal-EHC based on Block Position in lower Triangle (EEBPT)

In the encryption process of EEBPT, the blocks which are in the index that pass the equation (Mod ((i+1)/ (j+1), 2)> 0), are encrypted with El-Gamal. In the other hand, the blocks are encrypted with EHC. In decryption process, the same way is followed. In this scheme, 3680 blocks are encrypted with El-Gamal cryptosystem and the remaining 656 blocks are encrypted with EHC. Figure 4 shows the EEBPT general steps.

Journal of Theoretical and Applied Information Technology
15th October 2018. Vol.96. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

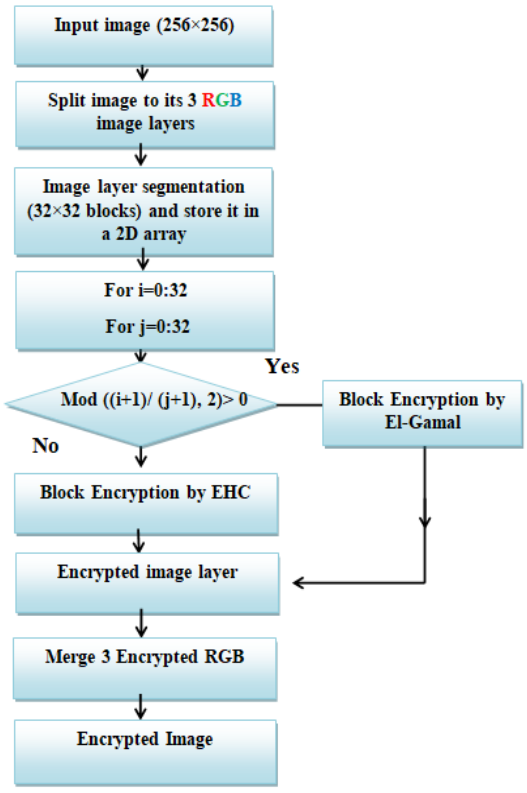

Figure 4: El-Gamal-EHC based on block position in lower Triangle (EEBPT)

The figure 5 below is illustrates that the blocks which are in red color are encrypted with El-Gamal and other blocks with EHC.

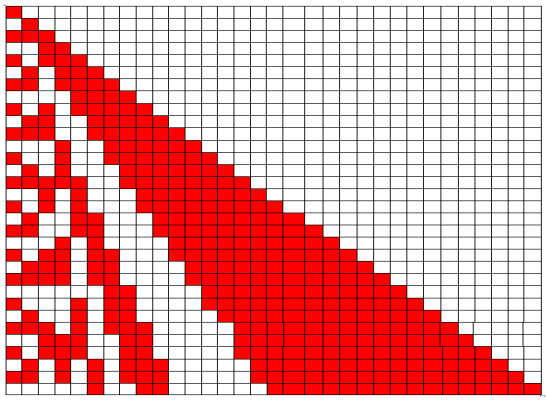

*Figure 5: Layer of image (32*32 blocks) encrypted with (EEBPT)*

3. El-Gamal-EHC based on Zigzag Scanning and Counter (EEZSC)

In EEZSC scheme, all the previous steps are the same, but in this scheme, zigzag scanning is used starting from the upper left corner of the two-dmensional array of blocks. The image's block is encrypted alternately in neighbouring blocks by the way of encrypting a block with El-Gamal and the next block with EHC.

The condition is should not exceed of 200 blocks which are encrypted with El-Gamal. Figure 6 shows the basic steps of EEZSC scheme.

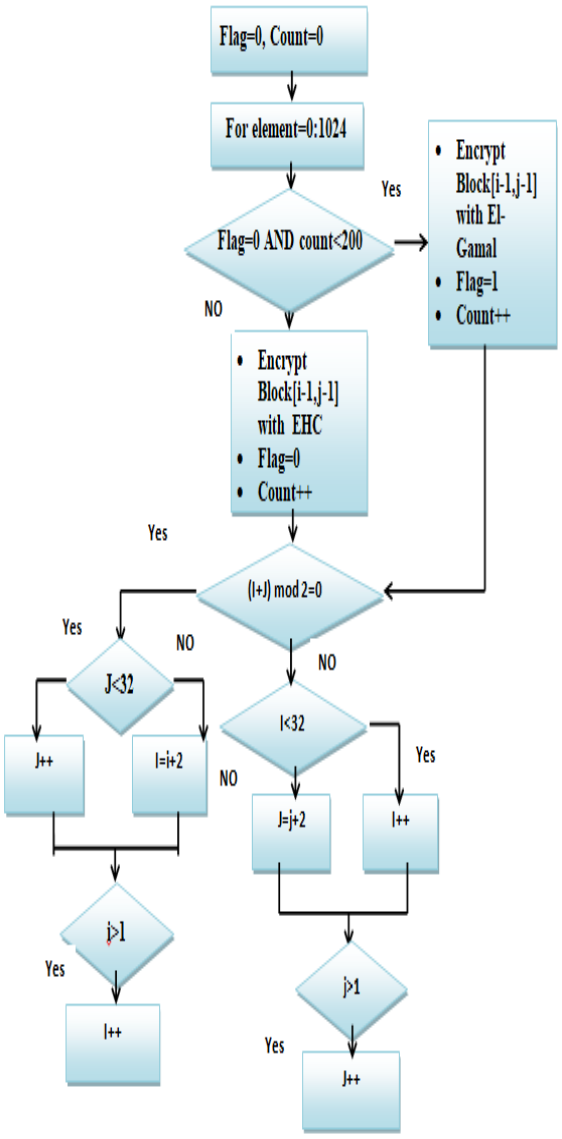

Figure 6: El-Gamal-EHC based on Zigzag Scan and Counter (EEZSC)

Journal of Theoretical and Applied Information Technology
15th October 2018. Vol.96. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

8. STATISTICAL TESTS

This section of study presented a number of quality metrics to examine the efficiency and performance of proposed scheme. The proposed methods have been tested on 800 images as database which collected manually from various web sites.

The statistical analysis is used to check the confusion and diffusion of the encrypted image's properties of the proposed system. To check how the proposed schemes are resists against statistical attack. Quality assessment is a very important stage to check the efficiency and effectiveness of cryptographic algorithms. There are many methods to assess cryptography techniques. The following image encryption quality metrics are used for evaluation [30], [31], [32] , [33].

1. **Peak Signal-to-Noise Ratio (PSNR) analysis**: is the ratio between plain image and cipher image and it is measured in a disciple. The higher value of PSNR is referring to the cipher image is closer to the plain image; therefore, for better encryption, the PSNR must be a lower value.

Equation (2) shows the Mean Squared Error (MSE). The MSE computes the difference between the plain and cipher images. Equation (3) shows PSNR which affect by MSE value.

$$MSE = \frac{1}{M \times N} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} [x(m,n) - x'(m,n)]^2 \quad (2)$$

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (3)$$

Table 1: PSNR between plain image and cipher image for all method

Images	PSNR db El-Gamal	PSNR db EHC	PSNR db EEOE	PSNR db EEBPT	PSNR db EEZSC
lene	7.3347	7.3323	7.3393	7.3356	7.3370
Pepper	7.3619	7.3518	7.3595	7.3528	7.3571
Baboon	7.4399	7.4516	7.4481	7.4408	7.4514

The results of PSNR for the methods are very closed, that mean the encrypted images takes the characterization of two hybrid methods El-Gamal and EHC together.

2. Correlation Coefficient Analysis (see equation 4): is used to evaluate the quality of the encryption. The higher correlation images, the closer correlation coefficient value to 1 should be occurred. In other hand, for encrypted images, the closer correlation coefficient value to 0 that means the lower correlation between cipher and plain images.

$$Corr = \frac{\sum_{r=1}^{N} \sum_{c=1}^{N} (I_1(r,c) - I\prime_1)(I_2(r,c) - I\prime_2)}{\sqrt{[\sum_{r=1}^{N} \sum_{c=1}^{M} (I_1(r,c) - I\prime_1)^2][\sum_{r=1}^{N} \sum_{c=1}^{M} (I_2(r,c) - I\prime_2)^2]}} \quad (4)$$

Table 2: Correlation results for all methods.

	El-Gamal		
Image	**Vertical**	**Horizontal**	**Diagonal**
Lena	0.0044	-0.0071	0.0294
Pepper	-0.0029	0.0017	0.0085
Baboon	-0.0110	-0.0079	-0.0406
	EHC		
Image	**Vertical**	**Horizontal**	**Diagonal**
Lena	-0.1404	-0.0148	0.02607
Pepper	-0.1327	0.0367	-0.0246
Baboon	-0.1286	-0.0026	0.0116
	EEOE		
Image	**Vertical**	**Horizontal**	**Diagonal**
Lena	-0.0668	-0.0083	-0.0125
Pepper	-0.0741	0.0214	-0.0111
Baboon	-0.0687	-0.0101	-0.0315
	EEBPT		
Horizontal	**Diagonal**	**Horizontal**	**Diagonal**
-0.0138	0.0200	-0.0138	0.0200
0.0186	-0.0236	0.0186	-0.0236
-0.0034	-0.0056	-0.0034	-0.0056
	EEBPT		
Image	**Vertical**	**Horizontal**	**Diagonal**
Lena	-0.1125	-0.0185	-0.0155
Pepper	-0.1067	0.0316	-0.0125
Baboon	-0.1067	-0.0039	0.0138

The correlation results is very close to 0 that mean the proposed methods is very efficient like El-Gamal and EHC.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. Entropy is the expected value (or average of information) that can be extracted from the message, and expressed by equation (5).

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i) \quad (5)$$

Table 3: Entropy results for plain image ,El-Gamal and EHC

Images	*Entropy(bit) Plain image*	*Entropy(bit) cipher image El-Gamal*	*Entropy(bit) cipher image EHC*
Lena	7.2454	6.4150	6.4556
Pepper	7.5729	6.4016	6.4380
Baboon	7.3794	6.4595	6.5010

Table 4: Entropy results for proposed methods

Images	*Entropy(bit) cipher image EEOE*	*Entropy(bit) cipher image EEBPT*	*Entropy(bit) cipher image EEZSC*
Lena	6.3845	6.2993	6.4365
pepper	6.3765	6.2937	6.4192
Baboon	6.4173	6.3094	6.4703

Results show the proposed cryptosystems gave values close to original image entropy values (close to eight), means information leakage by proposed methods is very little.

4. **The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI):** NPCR is the average change in image's pixels between the encrypted image and the original image whenever the value is high and close to 99% were better. The unified average changing intensity (UACI) measures the average intensity of the differences between the original image and the encrypted image. NPCR and UACI of plain and cipher images are defined in equations (6, 7, and 8).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \quad (6)$$

$D\ (i, j)$ defined as:

$$D(i,j) = \begin{cases} 1 \ if \ c_1(i,j) = c_2(i,j) \\ 0 \ if \ c_1(i,j) \neq c_2(i,j) \end{cases} \quad (7)$$

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100 \quad (8)$$

Table 5: NPCR results for all methods

Images	*NPCR El-Gamal*	*NPCR EHC*	*NPCR EEOE*	*NPCR EEBPT*	*NPCR EEZSC*
Lena	99.7085	99.8825	99.8123	99.8107	99.8489
pepper	99.8413	99.9298	99.8672	99.8855	99.9130
Baboon	99.7055	99.8687	99.7924	99.8291	99.8336

As shown in Table (5), the values are greater than 99%, which is very good for all proposed methods. This means that the encrypted image is not associated with the original image and the amount of difference is very large, making it resistant to the deferential attack.

Table 6: UACI results for all methods

Images	*UACI El-Gamal*	*UACI EHC*	*UACI EEOE*	*UACI EEBPT*	*UACI EEZSC*
Lena	36.7715	36.8010	36.7568	36.7741	36.7837
pepper	38.2859	38.2512	38.2482	38.2391	38.2759
Baboon	35.8122	35.6500	35.6664	35.6892	35.6840

As shown in Table (6), the values of UACI for all proposed methods are closed to El-Gamal and EHC algorithms values. The ideal value of UACI is 33% if greater than Ideal value it is not suitable.

5. Time: In all Internet services, including cloud services, time is critical for users, especially

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in uploading and uploading digital files such as images. In the proposed algorithms, fair results have been obtained in terms of time compared to the El-Gamal and EHC algorithms.

Table 7: Time results for all methods

	El-*Gamal*		*EHC*	
Encryption Time/s	Decryption Time/s	Decryption Time/s	Encryption Time/s	Decryption Time/s
0.4086	0.3054	0.3490	0.4086	*0.3054*
0.4077	0.2998	0.3520	0.4077	*0.2998*
0.5046	0.3290	0.3579	0.5046	*0.3290*
	EEBPT		*EEZSC*	
Image	Encryption Time/s	Decryption Time/s	Encryption Time/s	Decryption Time/s
Lena	0.4621	0.3146	0.4230	0.3024
Pepper	0.4585	0.3103	0.4119	0.2987
Baboon	0.4754	0.3123	0.4240	0.2996

6. Environment Experimental: This Section deals with software and hardware characteristics which used in the experimental environment. The proposed security framework is designed using Java as programming language and NetBeans IDE 8.2 software in 64-bit system with 2.60 GHz core i7 processor and 8.00 GB of RAM, run with MS Windows 10 operating system. All this features are affecting the speed of execution.

9. CONCLUSION AND FUTURE WORK

This paper, explained a way of secure the digital images on public cloud which uses the hybrid homomorphic cryptosystem including El-Gamal and EHC. The proposed methods (EEOE, EEBPT, and EEZSC) give better results in term of time and security compared with the two previous methods.

The result of vertical, horizontal and diagonal correlation is close to 0 so the pair adjacent pixels not related to each other. The entropy values for cipher images through proposed image encryption algorithm not far from original image value, which means the pixels of cipher image, are independent of each other statistically, so it is difficult to deduce information from cipher image.

For differential attacks (NPCR, and UACI) the results shows that the proposed methods are resist these differential attacks effectively; a small modification in one pixel of the original image can cause big modification in the cipher image. The attacker may try to find the correlation between the original image and cipher image through small changes in cipher image. If it leads to a great change in the cipher image, then the differential attacks will fail to extract meaningful information from cipher image in depending on statistical ways.

The computed results of PSNR are less than 8dB. However, the lower PSNR values reflect the difficulty to reconstruct the original image from the cipher one. Finally, the speed of encryption algorithm is significant criterion of any system especially in real time application.

The proposed methods gave significantly better results than the related work in image encryption using other homomorphic techniques (RSA, *Paillier and the hybrid of RSA and Paillier*). Tables (8, 9 and 10) show evaluation results of related works [14].

Images	PSNR (db) (original, cipher image)	Entropy(bit)		NPCR	UACI	Time for encryption and decryption (sec)
1	6.9698	plain	7.4609	0.9388	0.3721	48.9371
		cipher	5.6003			
2	4.2949	plain	6.8662	0.9940	0.5374	48.1145
		cipher	5.0348			
3	6.4383	plain	7.5859	0.8618	0.3882	34.4409
		cipher	5.4709			

Table 8: Results Of Encryption Analysis Using RSA Image Encryption Algorithm

Table 9: Results of Encryption Analysis using Paillier Image Encryption Algorithm

Images	PSNR(dB) (original image, cipher image)	Entropy(bit)		NPCR	UACI	Time for encryption and decryption(sec)
1	4.3700	plain	7.5771	0.9560	0.5727	3680.396
		cipher	3.232			
2	2.3477	plain	6.8652	0.9427	0.7226	6829.033
		cipher	3.6794			
3	4.6757	plain	7.6203	0.9999	0.5233	4019.477
		cipher	3.6572			

Table 10: Results of Encryption Analysis using Hybrid RSA and Paillier

Images	PSNR(dB) (original image, cipher image)	Entropy(bit)		NPCR	UACI	Time for encryption and decryption(sec)
1	7.0194	Plain	7.4609	0.9322	0.3739	208.2161
		Cipher	6.1473			
2	4.8538	Plain	6.8662	0.9484	0.4797	322.3505
		Cipher	6.0997			
3	6.9395	Plain	7.5859	0.9292	0.3690	344.3505
		Cipher	6.1499			

In future work will aim to expand the proposed system in order to obtain an integrated security system for the protection of multimedia types such as text files, audio and video. In other hand, Improve the performance and security of the proposed system through the use of other encryption techniques to encrypt images as well as digitally signed.

In addition, we will work on the authentication of encrypted image using steganography and hash function to ensure integrity of image and user authentication.

REFERENCES

[1] Peter Mell , Timothy Grance, "The NIST definition of cloud computing," *Special Puplication 800-145,* september 2011.

[2] Dimitrios Zissis , Dimitrios Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems 28 (2012) 583–592,ELSEVIER,* 2012.

[3] Subhadra Bose Shaw,Dr. A.K.Singh, "A Survey on Cloud Computing," *Green Computing Communication and Electrical Engineering (ICGCCEE),IEEE International Conference on,* 2014.

[4] Yashpalsinh Jadeja , Kirit Modi, "Cloud Computing - Concepts, Architecture and Challenges," *Intenational Conference on Computing, Electronics and Electrical Technologies [ICCEET],* 2012.

[5] M. Thangavel, P. Varalakshmi, S. Renganayaki, G.R. Subhapriya, T. Preethi, A. Zeenath Banu, "SMCSRC - Secure Multimedia Content Storage and Retrieval in Cloud," *FIFTH INTERNATIONAL CONFERENCE ON RECENT TRENDS IN INFORMATION TECHNOLOGY,* 2016.

[6] Aloka Sinha, Kehar Singh, "A technique for image encryption using digital signature," *Optics Communications 218 (2003) 229-234,* 2003.

[7] Alexander Edi Suranta Kacaribu, Ratnadewi, "Multiplying Cipher Images on Visual Cryptography with ElGamal Algorithm," *Int. Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), Indonesia, IEEE,* 2015.

[8] Xinpeng Zhang, Guorui Feng, Yanli Ren, Zhenxing Qian, "Scalable Coding of

Encrypted Images," *IEEE,* 2012.

[9] Chunhe Song, Xiaodong Lin, Xuemin (Sherman) Shen, "Secure and Effective Image Storage for Cloud Based E-healthcare Systems," *Communication and Information System Security Symposium,IEEE,* 2013.

[10] Bin Pan, Yu Tian, Tian-shu Zhou, Feng Wang, Jing-song Li, "Study on Image Encryption Method in Clinical Data Exchange," *International Conference on Information Technology in Medicine and Education,IEEE,* 2015.

[11] Anusha Bilakanti, Anjana.N.B,Nilotpal Chakraborty,G. K. Patra, "Secure Computation over Cloud using Fully Homomorphic Encryption," *IEEE,* 2016.

[12] J. Z. Y. L. O. C. A. Yunyu Li, "Reducing the Ciphertext Expansion in Image Homomorphic Encryption via Linear Interpolation Technique," *Global Conference on Signal and Information Processing (GlobalSIP),IEEE ,* 2015 .

[13] P. P. Gajendra Singh Chandel, "Image Encryption with RSA and RGB randomized Histograms," *International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering,* 2014.

[14] H. A. Y. Huda M. Saleh, "Private Searching on Encrypted Data in Cloud," *International Journal of Computer Applications (0975 – 8887),* 2017.

[15] Geetha V, Laavanya N, Priyadharshiny S, Sofeiyakalaimathy C, "Survey on Security Mechanisms for Public Cloud Data," *IEEE,* 2016.

[16] Annapoorna Shetty, Shravya Shetty K, Krithika K, "A Review on Asymmetric Cryptography –RSA and ElGamal Algorithm," *International Journal of Innovative Research in Computer and Communication Engineering,* 2014.

[17] Passent M. El-Kafrawy, Azza A. Abdo, Amr. F. Shawish, "Security Issues Over Some Cloud Models," *International Conference on Communication, Management and Information Technology (ICCMIT),ELSEVIER,* 2015.

[18] H. Tianfield, "Security Issues In Cloud Computing," *IEEE International Conference on Systems, Man, and Cybernetics,* 2012.

[19] Dimitrios Zissis , Dimitrios Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems, ELSEVIER,* 2012.

[20] Nitin Jain, Saibal K. Pal ,Dhananjay K. Upadhyay, "Implementaion and analysis of homomorphic encryption schemes," *International Journal on Cryptography and Information Security(IJCIS) ,* 2012.

[21] C. H. Dagli, "Homomorphic Encryption," *Procedia Computer Science ,ELSEVIER,* 2013.

[22] Ryan Hayward , Chia-Chu Chiang, "Parallelizing fully homomorphic encryption for a cloud environment," *Journal of Applied Research and Technology,* 2015.

[23] RatnaKumari Challa, G. VijayaKumari, Sunny B, "Secure Image processing using LWE Based Homomorphic Encryption," *IEEE,* 2015.

[24] Khalid EL MAKKAOUI, Abdellah EZZATI,Abderrahim BENI HSSANE, "Challenges of Using Homomorphic Encryption to Secure Cloud Computing," *IEEE,* 2015.

[25] Prashant Sharma, Sonal Sharma, Ravi Shankar Dhakar, "Modified Elgamal Cryptosystem Algorithm (MECA)," *International Conference on Computer & Communication Technology (ICCCT),IEEE,* 2011.

[26] T. ELGAMAL, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE TRANSACTIONS ON INFORMATION THEORY,* 1985.

[27] A. R. Z. M. A. A. Amer Daeri, "ElGamal public-key encryption," *International Conference on Control, Engineering & Information Technology (CEIT'14),* 2014.

[28] By Gorti VNKV Subba Rao, Dr. Garimella Uma, "An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme," *Global Journal of Computer Science and Technology Network, Web & Security,* 2013.

[29] Gorti VNKV Subba Rao, Md.Sameeruddhin Khan, Mr.A.Yashwanth Reddy, Mr.K.Narayana , "Data Security in Bioinformatics," *International Journal of*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Advanced Research in Computer Science and Software Engineering, 2013.

[30] H. M. Al-Mashhadi, "Quality Assessment for Image Encryption Techniques using Fuzzy Logic System," *International Journal of Computer Applications (0975 – 8887),* 2017.

[31] A.M. Vengadapurvaja, G. Nisha, R. Aarthy, N. Sasikaladevi, "An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security," *7th International Conference on Advances in Computing & Communications, ICACC,ELSEVIER,* 2017.

[32] N. Sethi, "Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique," *Conference on Advances in Communication and Control Systems* , 2013.

[33] Haider M. Al-Mashhadi, Iman Q. Abduljaleeian, " Color Image Encryption using Chaotic Maps, Triangular Scrambling, with DNA Sequences," *International Conference on Current Research in Computer Science and Information Technology (ICCIT), IEEE* , 2017.