Hybrid Homomorphic Cryptosystem for Secure Transfer of Color Image on Public Cloud

Haider M. Al-Mashhadi† and Ala'a A. Khalf ††

Information System Dept., College of Information Technology, University of Basra, Basra, Iraq
Computer Science Dept., College of Science,, University of Basra, Basra, Iraq

Summary
Cloud computing is a model of advanced computing which has a strong impact on information technology. Cloud computing provides remote accessing to shared digital resources in the stored cloud. Practically on cloud servers using Web services that provide a huge benefits to the user in various applications such as social networking, banking, finance, storage and e-mail, and achieve many features related to flexibility, ease of use, reliability and performance with high and low cost. Cloud computing gives opportunity to the users to upload and offload data to the cloud using client devices i.e. mobile applications. There are some potential concerns related to security and privacy with cloud computing because cloud systems are usually in a public domain. 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 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.

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

2. Literature survey

The researchers in [7] uses partial homomorphic encryption based on El-Gamal scheme to achieve image security and then explained how to multiply many of cipher images so that it will be more resist to cracking. The statistical test MSE (Mean Squared Error) is used to compare between the original image and decrypted image for checking errors detection. The Results of MSE test is equal to 0 this means the original image and decrypted image is exactly identical.

The researchers in [8] proposes a new technique of scalable coding for encrypted images. In the encryption stage, the pseudorandom numbers which are derives from a private key are masked by a modulo-256 addition with original pixels of image. Then they quantize the encrypted image with hadamard coefficients.

In [9] the authors present a chaotic cryptosystem for image encryption that provide low computation complexity. In this proposed method the encryption

Manuscript received March 5, 2018
Manuscript revised March 20, 2018

process is implemented in the client equipment. A new lossy compression technique for encrypted image is proposed, which is based on the compressive sensing CS.
The article in [10] in their method they use RSA, AES and Murmur-Hash. The method encrypts the pixels with RSA and AES separately, and to achieve image integrity, Murmur-Hash is embedded in encrypted image thus improving both of security and performance. The encrypted image is also decrypted without any loss of information.
Other proposed encryption method shows in [11] proposed fully homomorphic cryptosystem which is based on the learning with errors (LWE) problem. Their method is a modified scheme from the BVG cryptosystem for image encryption that provide less computations over the cloud. In this scheme, they modify basic LWE based FHE to process decimal inputs directly as described in BGV cryptosystem.

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 [12]. 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: [13]

1) Authentication: is intended to verify user identity. Identity and authentication management is concerned with preventing unauthorized persons from accessing IT resources [14].
2) Confidentiality: means that protected data is only accessed by authorized persons who have permission access to the protected data. [15].
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 [16].
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 [17]. 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 [18]. 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. [19]. 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 [20]. Homomorphic cryptosystems are classified to three models according to the operations that performed on the data [21]:

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.

4.1 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 [22]:

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 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 [23]. In other hand, El-Gamal cryptosystem need for randomness that make 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 [24].

4.2 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 is explained in the algorithm (2) below [25].

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**:** [26]

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.

5. Proposed method

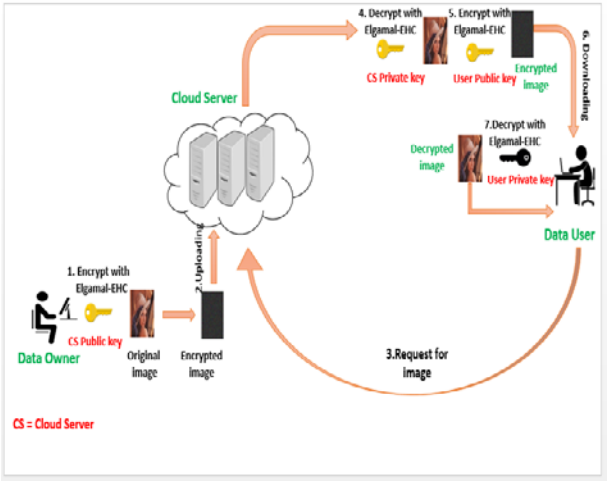

Fig.1 Proposed method mechanism

Fig. 1, illustrate the proposed method mechanism; Images of data owner are encrypted with El-Gamal-EHC according to public key cloud server. The encrypted image will be uploaded to store it in cloud server, when user requests an image that is stored in server as encrypted form. The cloud server will decrypt demand image with his private key and encrypt the image again with user's public key. Then the cloud sends the encrypted image to the user. The final encrypted image is decrypted by the user according to the user's private key. This process will

secure the encrypted image from alteration which causes by an authorized user in man in the middle attack. 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 fig. 2.
- El-Gamal-EHC based on *block position in lower Triangle (EEBPT)*, the algorithm of this method shown in fig.3.
- El-Gamal-EHC based on Zigzag Scan and Counter (EEZSC), the algorithm of this method shown in fig.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.

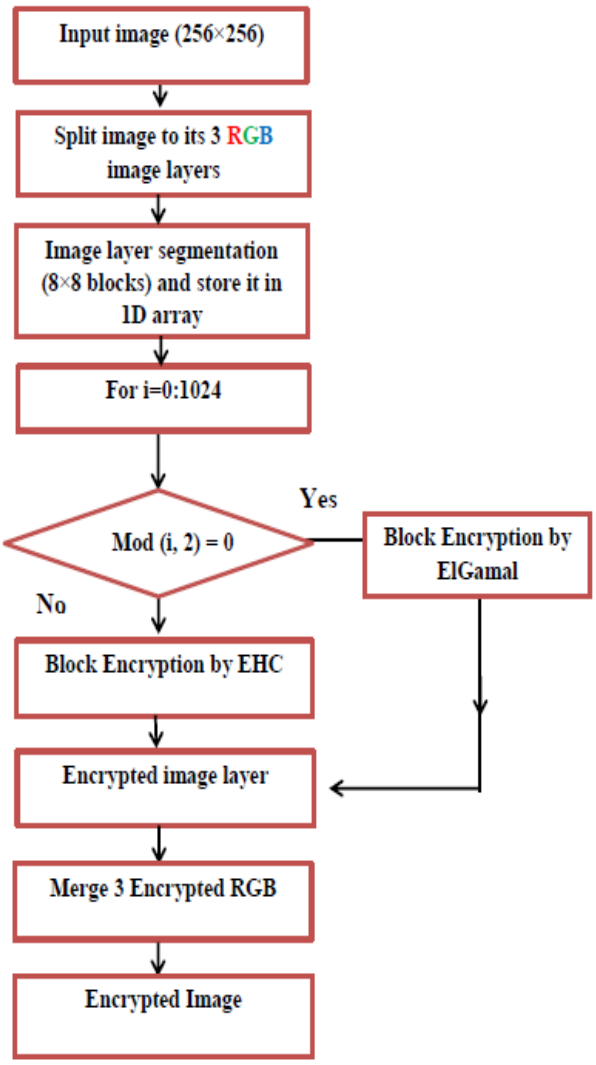

Fig.2 El-Gamal-EHC based on Odd and Even block index (EEOE)

Fig 2, the original image is separated into three channels: red, green and blue. The channels are divided into 1024 blocks which have 8 * 8 pixels. The resulted blocks are stored in a vector. In the encryption process, the blocks with even index are encrypted with El-Gamal. However, the blocks with odd index are encrypted with EHC. The same indices are considered in decryption process.

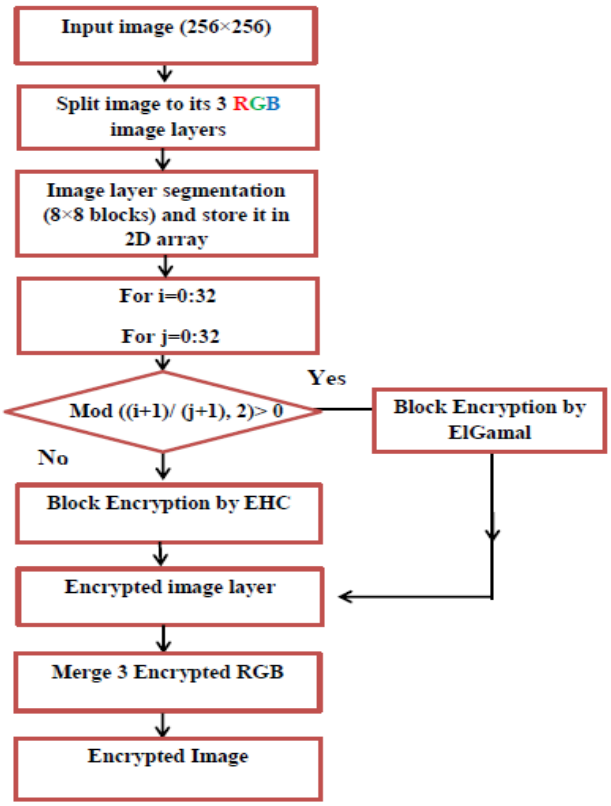

Fig.3 El-Gamal-EHC based on block position in lower Triangle (EEBPT)

In Fig. 3, the original image is separated into three channels: red, green and blue. The channels are divided into 1024 blocks which have 8 * 8 pixels. The resulted blocks are stored in a two-dimensional array. In the encryption process, the blocks which are in index that pass the equation (1)

$$f = (i+1)/(j+1) \bmod 2 \qquad (1)$$

If the value of f greater than 0 then the algorithm encrypts the current block using El-Gamal method otherwise encrypts the current block using EHC method. In this scheme 368 blocks are encrypted with El-Gamal cryptosystem and the remaining 656 blocks are encrypted with EHC. Fig. 4, illustrates that the blocks which are in red colour is encrypted with El-Gamal and other blocks with EHC.

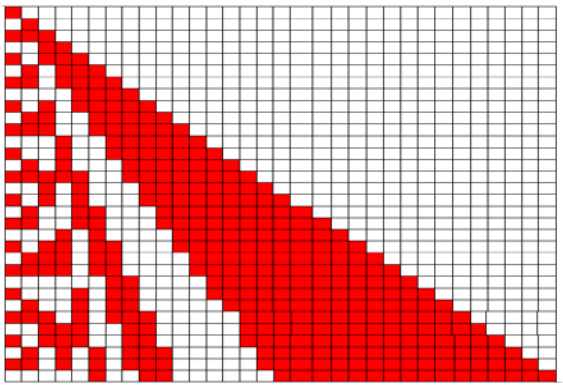

Fig. 4 Layer of image (32*32 blocks) encrypted with (EEBPT).

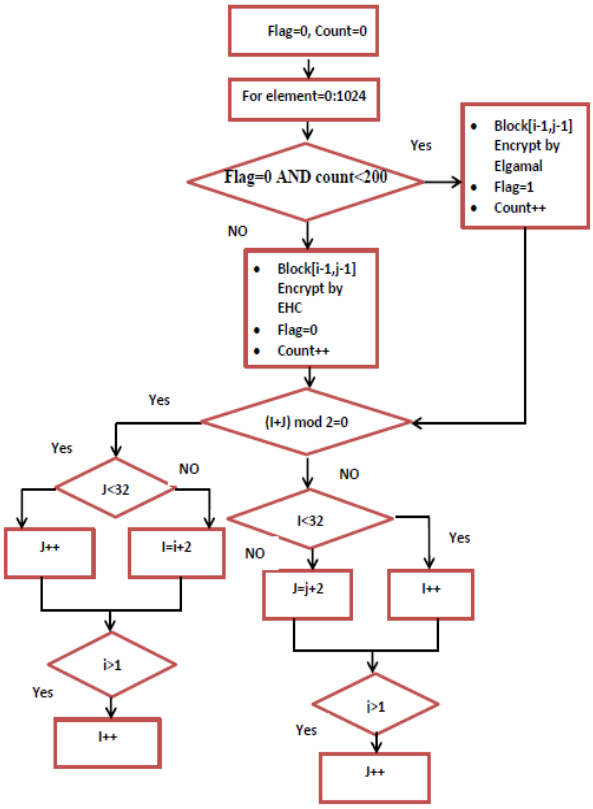

Fig. 5 El-Gamal-EHC based on Zigzag Scan and Counter (EEZSC)

Fig. 5 follows the steps in fig 2 and fig 3.However, the code is zigzag scanning which start from the upper left corner of the two dimension array of blocks. Note that, the blocks are encrypted with El-Gamal should not exceed of 200 blocks, while the rest of blocks encrypts by EHC scheme.

6. Statistical tests

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 [27], [28], [29] , [30].

6.1 PSNR Peak Signal-to-Noise Ratio is the ratio between plain image and cipher image and it is measured in disciple. The higher value of PSNR is refers to the cipher image is closer to plain image; therefore, for better encryption the PSNR must be lower value.
Equation (2) shows the mean the average 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 methods

Images	PSNR db El-Gamal	PSNR db EHC	PSNR db EEOE	PSNR db EEBPT	PSNR db EEZSC
Lena	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.

6.2 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.

$$Corr = \frac{\sum_{r=1}^{N} \sum_{c=1}^{N} (I_1(r,c) - I'_1)(I_2(r,c) - I'_2)}{\sqrt{[\sum_{r=1}^{N} \sum_{c=1}^{M} (I_1(r,c) - I'_1)^2][\sum_{r=1}^{N} \sum_{c=1}^{M} (I_2(r,c) - I'_2)^2]}} \quad (4)$$

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		
Image	**Vertical**	**Horizontal**	**Diagonal**
Lena	-0.0921	-0.0138	0.0200
Pepper	-0.0876	0.0186	-0.0236
Baboon	-0.0882	-0.0034	-0.0056

	EEZSC		
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.

6.3 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 all methods

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

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

The results show that the proposed cryptosystems gave entropy values that do not leak information.

6.4 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 4: 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

Table 5: 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

6.5 Time: In all Internet services, including cloud services, time is critical for users, especially in uploading and down loading 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 6: Time results for all methods

	El-Gamal		*EHC*	
Image	Encryption Time/s	Decryption Time/s	Encryption Time/s	Decryption Time/s
Lena	0.5774	0.3490	0.4086	0.3054
Pepper	0.5781	0.3520	0.4077	0.2998
Baboon	0.5712	0.3579	0.5046	0.3290

	EEOE	
Image	Encryption Time/s	Decryption Time/s
Lena	0.5503	0.3707
Pepper	0.5620	0.3483
Baboon	0.5627	0.3536

	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

7 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, because they take the good characteristics of El-Gamal and EHC methods like very good security and small run time executions. In future work 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] Geetha V, Laavanya N, Priyadharshiny S, Sofeiyakalaimathy C, "Survey on Security Mechanisms for Public Cloud Data," IEEE, 2016.
[13] 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.
[14] 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.
[15] H. Tianfield, "Security Issues In Cloud Computing," IEEE International Conference on Systems, Man, and Cybernetics, 2012.
[16] Dimitrios Zissis , Dimitrios Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, ELSEVIER, 2012.
[17] Nitin Jain, Saibal K. Pal ,Dhananjay K. Upadhyay, "Implementaion and analysis of homomorphic encryption schemes," International Journal on Cryptography and Information Security(IJCIS) , 2012.
[18] C. H. Dagli, "Homomorphic Encryption," Procedia Computer Science ,ELSEVIER, 2013.
[19] Ryan Hayward , Chia-Chu Chiang, "Parallelizing fully homomorphic encryption for a cloud environment," Journal of Applied Research and Technology, 2015.
[20] RatnaKumari Challa, G. VijayaKumari, Sunny B, "Secure Image processing using LWE Based Homomorphic Encryption," IEEE, 2015.
[21] Khalid EL MAKKAOUI, Abdellah EZZATI,Abderrahim BENI HSSANE, "Challenges of Using Homomorphic Encryption to Secure Cloud Computing," IEEE, 2015.
[22] Prashant Sharma, Sonal Sharma, Ravi Shankar Dhakar, "Modified Elgamal Cryptosystem Algorithm (MECA)," International Conference on Computer & Communication Technology (ICCCT),IEEE, 2011.
[23] T. ELGAMAL, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE TRANSACTIONS ON INFORMATION THEORY, 1985.
[24] A. R. Z. M. A. A. Amer Daeri, "ElGamal public-key encryption," International Conference on Control, Engineering & Information Technology (CEIT'14), 2014.
[25] 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.
[26] Gorti VNKV Subba Rao, Md.Sameeruddhin Khan, Mr.A.Yashwanth Reddy, Mr.K.Narayana , "Data Security in Bioinformatics," International Journal of Advanced Research in Computer Science and Software Engineering, 2013.
[27] H. M. Al-Mashhadi, "Quality Assessment for Image Encryption Techniques using Fuzzy Logic System," International Journal of Computer Applications (0975 – 8887), 2017.
[28] 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.
[29] N. Sethi, "Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique," Conference on Advances in Communication and Control Systems , 2013.
[30] 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.