[Leela, 3(8): August 2016]
DOI-10.5281/zenodo.59610

ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURED CHANGE DETECTION OF SATELLITE IMAGES USING HOMOMORPHIC ENCRYPTION

Leela.S [1], P.Nithyanandam [2]

[1] Research Scholar, VIT University, Chennai Campus

[2] Professor VIT University, Chennai Campus

ABSTRACT

Satellite images are used in determining the dynamic state of the earth surface (viz., land, water, forest etc.,) for each and every moment. Detecting geographical changes on the earth surface using satellite images is crucial in several applications. With the increasing research in geographical sciences and technologies, there is a huge demand for the privacy and security of these satellite images when they are stored and processed at a remote server. There is a necessity to ensure privacy and enable computations on private data and images located and processed by an untrusted remote server. The goal is to delegate the processing of data without giving away access to it. Homomorphic encryption algorithms are used to attain such special requirements. This paper proposes a research work on practical implementation of change detection from one image with the other using image differencing technique on encrypted images which are processed by an unsecured remote server. Paillier encryption scheme is proved to be secured and applicable for Homomorphic operations. Paillier algorithm is implemented to examine the Homomorphic operations on encrypted grayscale images. The correctness of the algorithm is verified by encryption, decryption and evaluation function.

Keywords- Homomorphic Image Encryption, Paillier encryption, Change detection, Image encryption/decryption, Satellite image processing, Image security.

I. INTRODUCTION

In the recent times, satellite image processing techniques are widely used to monitor the geographical changes, land cover changes, deforestation, urban growth, changes over time, disaster effects and also for the military purposes. All of these applications are intend to analyse the dynamic changes that happen on the earth surface from time to time [1]. Change detection methods are basically of two types. They are supervised methods and unsupervised methods. An unsupervised method is used in this paper to observe change detection by directly comparing two satellite images. Some of the unsupervised change detection methods are as follows: Image differencing algorithm, Wavelet transformation, Change vector analysis, Principal component analysis (PCA) and Image rationing [14]. Most of the unsupervised methods are developed based on the image differencing technique [7]. Image differencing algorithm performs pixel wise subtraction on two input images that are taken for analysis. These images are captured at two different time instances of a same geographical location. The image differencing algorithm produces a new image called difference image. The time difference of two image acquisition may vary from few minutes to few years in real time image processing [16]. The computed difference image contains the values of the pixels associated with land cover changes present values significantly distinct from those of the pixels associated with unchanged areas.

When the geographical satellite images owned by an organization/individual are to be transferred to the cloud server with a constraint of secure storage, we use standard encryption methods to protect the sensitive data. But when we want to carry out some processing on the image placed on a remote server, it is necessary that the cloud provider has to be given access to the unencrypted version of the stored image. When we want to process the highly confidential images without compromising privacy and security, we download the images from the cloud, decrypt it; perform image processing operations on the image and then encrypt and store it back in the cloud. This makes the task cumbersome since the up and down image transmission, encryption/decryption operation should happen for every computation. So the cloud provider gets the access to the raw image and do the processing on it. But in this case we lose our privacy towards the sensitive images. Due to limited computing power of resources available with us, we are in a position to delegate data processing to the cloud service even though it is not trustable. To address this issue, a

ISSN 2348 – 8034
Impact Factor- 4.022

mechanism should be devised in such a way that the data has to be processed by the cloud server without giving access to data it process. Homomorphic encryption helps us to delegate processing while preserving privacy of data [3]. Adaption of Homomorphic Encryption algorithms in this context allows all image processing operations on the confidential images with the complete control of the user/owner. However, the research on Homomorphic Encryption is not matured yet [19].

In this paper, for an image processing application, i.e. a secured change detection technique is proposed by subtracting the two encrypted satellite images. The two grayscale satellite images captured from the same area but at two different time instances are encrypted using Paillier's encryption algorithm. The pixel wise subtraction is carried out on the encrypted images. We apply the encryption algorithm on each pixel value of the input images to get the encrypted images. Then, pixel wise subtraction of encrypted images using the Paillier algorithm is done. As a result, a difference image which has the intensity differences of the two encrypted images is constructed. On every pixel of the difference image, decryption operation is carried out by using Paillier's decryption algorithm. Finally, we get the decrypted output image which has the subtracted intensity value between two input image taken for image differencing operation. The decrypted output image depicts that as if the subtraction operation was carried on the plain data. This is due to the characteristics of Paillier encryption algorithm. Hence the image differencing operation is applied on the encrypted images, the system ensures privacy and security.

II. PRELIMINARIES

A. Homomorphic Encryption

Homomorphic encryption algorithms are similar to conventional public key encryption algorithms with added functions and properties. A Standard Cryptographic Algorithm has the following three functions. KeyGen, Encrypt and Decrypt [18]. KeyGen is a Key generation Function which produces a pair of Secret key (Sk) and public key (Pk) based on some security constraints and parameters. Using public key Pk, Encryption algorithm converts the plain text message M to Cipher text C. Using secret key Sk, Decryption algorithm transforms cipher text C back to the plain text M. A Homomorphic encryption is a public key cryptosystem with an ability to perform the additional operations on the encrypted data [2]. Homomorphic Encryption consists of four functions: KeyGen, Encrypt, Evaluate and Decrypt [5]. Evaluation function is used to perform the operations on the encrypted data without using a Secret key. When we decrypt the result of evaluation algorithm, it gives the same result as if we had carried out the operation on the original messages. Homomorphic Encryption means an encryption is Homomorphic which permits computing on encrypted data [13]. For example, if the client uses the message M and produces the cipher text EM and send it to the server. The server now can use the cipher text EM and evaluate the function f on the underlying message M obtaining the encrypted result (f(EM)). The client can decrypt the result to get the result f(M) as an output [8]. Here the server performed the computation on the Client's encrypted data without knowing anything about the original data and without the knowledge of secret key. Since the processing is done on encrypted images, Homomorphic encryption ensures privacy and security.

Homomorphic encryption can be classified into somewhat Homomorphic encryption and Fully Homomorphic encryption [9]. Somewhat Homomorphic encryption is used in this paper. A somewhat Homomorphic encryption scheme supports limited number of addition operation and multiplication operation on the encrypted data [10]. An encryption scheme which supports any number of addition and multiplication operation is called fully Homomorphic scheme [4].

B. Properties of Homomorphic Encryption

Homomorphic Encryption possess two important properties [13]. If M is an additive (semi-)group, then the scheme is called additively Homomorphic. Otherwise, the scheme is called multiplicatively Homomorphic.

B. Additive Homomorphic Encryption

A Homomorphic encryption is additive, if:

$$E(M1 \oplus M2) = E(M1) \oplus E(M2) \quad (1)$$

M1 and M2 are the input plain text messages. E () is the encryption algorithm. C1 and C2 are the corresponding cipher texts produced by the encryption algorithm. D () is the decryption algorithm which converts the cipher text back to plain text. The encryption function is called as additively Homomorphic, if the product of two cipher texts will decrypt to the sum of their equivalent plaintexts [11],

$$(\mathrm{E}(\mathrm{M1}, \mathrm{r1}) . \mathrm{E}(\mathrm{M2}, \mathrm{r2}) \bmod n^2) = E(M1 + M2)\, mod\ n \quad (2)$$

Raise one of the plain text to g, then multiply it with the other cipher text. When we decrypt this product, we get the sum of plain texts. [11]

$$(\mathrm{E}(\mathrm{M1}, \mathrm{r1}) \cdot g^{M2} \bmod n^2) = E(M1 + \mathrm{M2}) \bmod \mathrm{n} \quad (3)$$

C. Multiplicative Homomorphic Encryption

A Homomorphic encryption is multiplicative, if the product of two cipher texts will decrypt to the product of their equivalent individual plaintexts [15].

ISSN 2348 – 8034
Impact Factor- 4.022

$$E(M1 \otimes M2 = E(M1) \otimes E(M2) \quad (4)$$
$$E(M1, r)k \ mod \ n^2 = E(k.M1) \ mod \ n \quad (5)$$

for every k ∈ Z_N. Here k is the multiplication factor.

III. PROPOSED WORK

A. Paillier Cryptosystem

The homomorphic cryptosystem was first introduced by Rivest *et al.* [11] as a privacy homomorphism, which is defined as an encryption function allowing one to operate the ciphertexts without decrypting them into plaintexts. Specifically, there exist two algebraic operations corresponding to each other, one in plaintext space and the other in ciphertext space. If M1 and M2 are any two plaintexts in Homomorphic cryptosystems, we have

$$D[E[M1] \circ E[M2]] = M1 \diamond M2 \quad (6)$$

Here $E[\cdot]$ is the encrypting operator and $D[\cdot]$ is the decrypting operator. Operators "∘" performs the algebraic operations in the ciphertexts and "◊" performs the algebraic operations in the plaintexts. The Paillier cryptosystem is a public key cryptosystem which has been proved to be semantically secure [2]. An exhaustive study of Paillier cryptosystem is observed below.

B. Key generation

Select two large prime numbers p and q randomly. Compute their product N and the least common multiple $\lambda(N)$ of $p-1$ and $q-1$, respectively. That is

$$N = p.q \quad (7)$$
$$\lambda(N) = \text{lcm}(p - 1, q - 1) \quad (8)$$

Randomly choose an integer $g \in Z^*_{N^2}$, where $Z^*_{N^2}$ denotes the subset of Z_{N^2} in which every element is relatively prime with N^2 and Z_{N^2} is the set of integers modulo N^2. (N, g) and λ are the public key and the private key, respectively.

C. Encryption

Let $m \in Z_N$ be a plaintext. The encryption process of m can be described as follows:

$$E[m, r] = g^m r^N \bmod N^2 \quad (9)$$

where $r \in Z^*_N$ is an integer chosen at random. According to the Paillier cryptosystem, the ciphertext C is in $Z^*_{N^2}$

D. Evaluation

Some useful homomorphic properties of the Paillier cryptosystem are

$$D[E[M1, r1]E[M2, r2] \bmod N^2] = (M1 + M2)mod \ n \quad (10)$$

$$D[E[M1, r1]E[(M2, r2)^{-1}] \bmod N^2] = (M1 - M2)mod \ n \quad (11)$$

$$D[E[M, r]^k \bmod N^2] = (k.M)mod \ n \quad (12)$$

E. Decryption

Let $C \in Z^*_{N^2}$ be the ciphertext. The decryption process of C can be described as follows:

$$D(C) = \{L(C^\lambda mod \ N^2 / L(g^\lambda \ mod \ N^2)\} \ mod \ N \quad (13)$$

where $L(\cdot)$ denotes the function $L(u) = (u - 1) / N$

F. Proposed Algorithm

The proposed algorithm for the secured image differencing is given below:

Step 1: Read two input images as matrices M1 and M2.
Setp 2: Compute Public key and Secret key for the Paillier cryptosystem.
Step 3: Encrypt matrices M1 and M2 to get C1 and C2 respectively by applying Paillier Encryption Public key.
Step 4: Calculate the multiplicative inverse of C2.
Step 5: Multiply C1 and the multiplicative inverse of C2
Step 6: Decrypt the product matrix by applying Paillier decryption Secret key.
Step 7: Display the decrypted result to see the difference image.

Figure1 describes the framework of the secured storage and processing of a sensitive data. It shows that the Homomorphic cryptosystem enables to do all the manipulation on encrypted images and helps to achieve the goal of privacy protection and secured computation.

ISSN 2348 – 8034
Impact Factor- 4.022

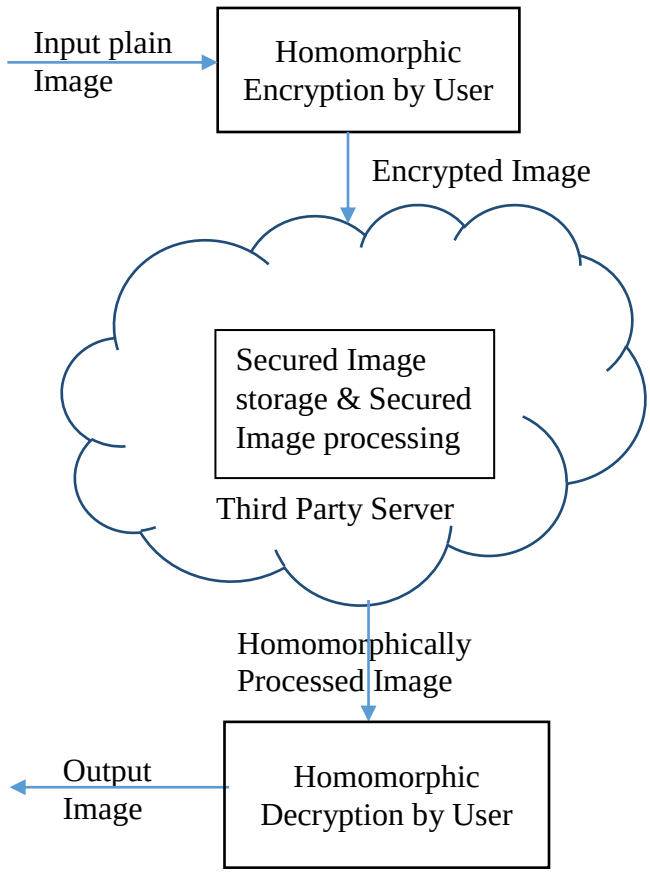


Figure1: Framework for secured image storage and processing

The step by step interpretation of the algorithm is demonstrated as follows. Let us take an example of a image matrix of size 2 x 2 and test the Homomorphic Image differencing operation.

$$M1=\begin{bmatrix}12 & 10\\ 42 & 15\end{bmatrix} M2=\begin{bmatrix}4 & 6\\ 18 & 15\end{bmatrix}$$

Create a message, M1, M2, with M ∈ ℤn. Let r = 23; Choose a random, nonzero integer, r ∈ $\mathbb{Z}^*_n$. Compute c ≡ $g^m \cdot r^N$ mod N^2. All the calculations are modular N^2 operations.

First, Encrypt M1 image matrix:

$$\cong\begin{bmatrix}(5652^{12}).(23^{77}) & (5652^{10}).(23^{77})\\ (5652^{42}).(23^{77}) & (5652^{15}).(23^{77})\end{bmatrix}$$

$$\cong\begin{bmatrix}(4404)(606) & (5303)(606)\\ (4019)(606) & (5655)(606)\end{bmatrix} mod\ N^2$$

$$\cong\begin{bmatrix}774\ mod\ 5929 & 100\ mod\ 5929\\ 4624\ mod\ 5929 & 5897\ mod\ 5929\end{bmatrix}$$

is the encrypted image matrix EM1.

Now, Encrypt image matrix M2:

$$\cong\begin{bmatrix}(5652^{4}).(23^{77}) & (5652^{6}).(23^{77})\\ (5652^{18}).(23^{77}) & (5652^{15}).(23^{77})\end{bmatrix}$$

$$\cong\begin{bmatrix}(2524)(606) & (5069)(606)\\ (1191)(606) & (5655)(606)\end{bmatrix} mod\ N^2$$

$$\cong\begin{bmatrix}5791\ mod\ 5929 & 592\ mod\ 5929\\ 4337\ mod\ 5929 & 5897\ mod\ 5929\end{bmatrix}$$

is the encrypted image matrix EM2.

Evaluation:
Let us do the differencing operation in the encrypted domain

$$\begin{bmatrix}8 & 4\\ 24 & 0\end{bmatrix}$$

is the difference image in plain domain.
Now the modulo inverse matrix $EM2^{-1}$ is calculated as,

$$\begin{bmatrix}(2363)\ mod\ 5929 & (2634)\ mod\ 5929\\ (3579) mod\ 5929 & (4632)\ mod\ 5929\end{bmatrix}$$

Now, multiply EM1 and $EM2^{-1}$

$$\begin{bmatrix}(774)(2363) & (100)(2634)\\ (4624)(3579) & (5897)(4632)\end{bmatrix} \text{mod } N^2$$

$$\begin{bmatrix}2830\ mod\ 5929 & 2524\ mod\ 5929\\ 1457\ mod\ 5929 & 1\ mod\ 5929\end{bmatrix}$$

Let us decrypt the above product matrix to get the plain domain subtraction matrix.

Decryption:

For any decryption with the public key (N, g), regardless of the value of C, the calculation of $g^{\lambda(N)}$ mod N^2 is necessary. This resulting value, an element of $\mathbb{Z}^*_{n^2}$, will, by Carmichael's Theorem, be congruent to 1 mod n. Thus, subtracting one from this resulting value will give a number that is divisible by n (congruent to zero mod n). So, we compute $g^{\lambda(n)}$ mod n^2, subtract one from this value, then divide that number by n.

λ(77) = lcm(6, 10) = 30

Define L(u) = (u – 1)/n

ISSN 2348 – 8034
Impact Factor- 4.022

Compute $L(g^{\lambda(n)} \bmod n^2) = k$

$L(5652^{30} \bmod 5929) = L(3928)$

Compute $L(g^{\lambda(n)} \bmod n2) = k$

$L(3928) = (3928 - 1)/77 = 3927/77 = 51$

Since $g^{\lambda(n)}$ is being calculated mod N^2 , it can be viewed as a number greater than or equal to zero, but strictly less than N^2, so dividing this number by N results in a value, k, greater than or equal to zero, but strictly less than N: $k \in \mathbb{Z}n$. Since $N = p \cdot q$, so long as k is not congruent to a multiple of p or q mod n, then k has an inverse, so $k \in \mathbb{Z}^*_n$. Values of g such that $L(g^{\lambda(n)} \bmod n^2)$ is congruent to a multiple of p or q mod n are the few exceptions of semi-random g values with orders divisible by N that must be excluded. If such a value is chosen, simply pick another value for g, and check that this property holds before publishing the public key. So, assuming k is not congruent to p or q mod N, then k has an inverse mod N, so compute $\mu = k^{-1} \bmod N$, For any decryption involving the public key (N, g), the value of μ will always be the same, and will always be necessary. So, Compute

$\mu \equiv k^{-1} \bmod N$ or else

$(\mu * k) \bmod N = 1 \bmod N.$

$51*74 \bmod 77 = 1 \bmod 77$. Thus $\mu=74$

To decrypt C1, one must calculate,

$M1 \equiv L(c^{\lambda(N)} \bmod N^2) \cdot \mu \bmod N$

$$\cong \begin{bmatrix} L(2830^{30}) & L(1457^{30}) \\ L(2524^{30}) & L(1^{30}) \end{bmatrix}$$

$$\cong \begin{bmatrix} (1772 \bmod 5929) & (5314 \bmod 5929) \\ (3851 \bmod 5929) & (1 \bmod 5929) \end{bmatrix}$$

Multiply it with μ mod N

$$\cong \begin{bmatrix} 23.74 \bmod 77 & 50.74 \bmod 77 \\ 69.74 \bmod 77 & 0 \end{bmatrix}$$

$$\cong \begin{bmatrix} 1702 \bmod 77 & 3700 \bmod 77 \\ 5106 \bmod 77 & 0 \end{bmatrix}$$

$$\cong \begin{bmatrix} 8 & 4 \\ 24 & 0 \end{bmatrix}$$

Now, we got the difference image matrix by decryption algorithm using the Homomorphic property of the Paillier algorithm. This result is same as the one that we obtained for plain text values.

Figure-2 gives the schematic of the Image subtraction operation on the Encrypted images. Key generation function takes two security parameters p and q and yields the publickey Pk and the Secret key Sk for the Paillier algorithm. M1 and M2 are the input images that are encrypted individually using the Public key Pk to produce cipher images C1 and C2 respectively. Pixel basis subtraction of one image from another image is performed by the third party server on cipher images. The difference image is then decrypted using Secret key Sk. Decryption algorithm is also applied on pixel by pixel. The output image will be same as the plain image subtraction.

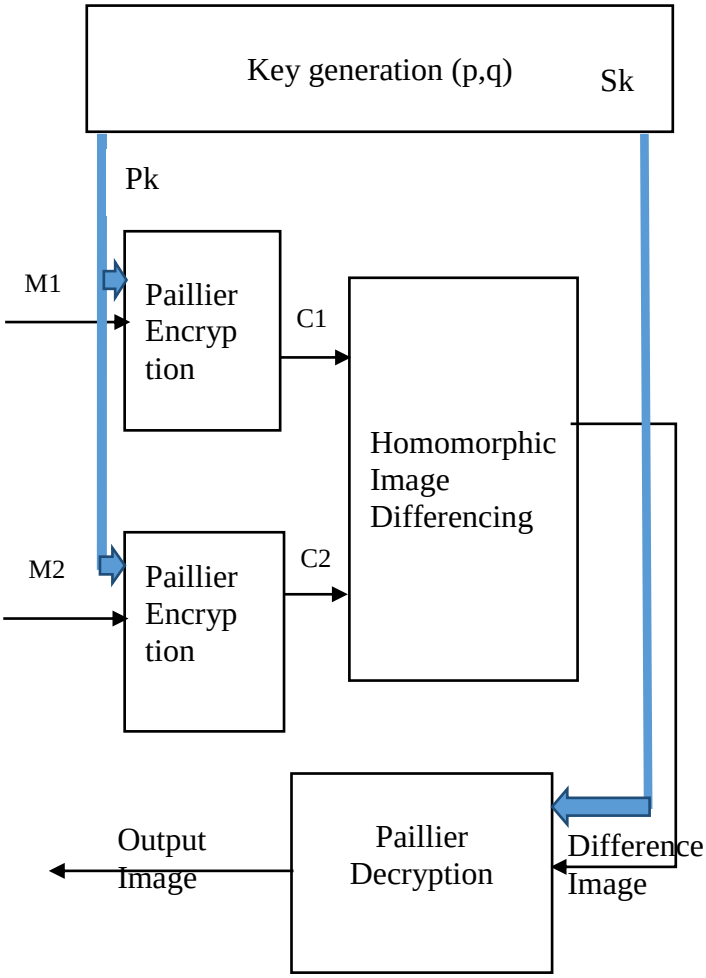


Figure2: Homomorphic image subtraction on images

IV. EXPERIMENTAL RESULTS AND OBSERVATIONS

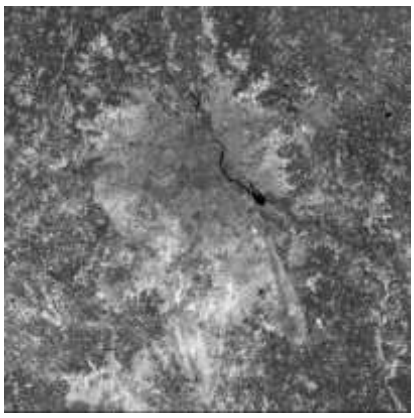
The Paillier algorithm is implemented based on the assumptions and properties of it. In a world becoming increasingly urbanized, India's capital New Delhi has seen growth dramatically. These Landsat images from March 1991 and March 2016 show the city and its

ISSN 2348 – 8034
Impact Factor- 4.022

adjacent suburban areas. The area's population is increased from 9.4 milliion to 25 million during that period. The United Nation's Report on World Urbanization projects that Delhi will be at 37 million residents by 2030. Landsat can be a valuable tool in monitoring the urban growth and its impact on the environment. New Delhi or any area that undergoes significant growth is a point to be discussed when it comes to urban planning. From a regional standpoint and also from a environmental stand point Landsat analysis is an important part of this. As we analyse these images, Homomorphic encryption operations are practically implemented to support image processing operations on the encrypted images. Figure 3 shows the Image subtraction operation on the Encrypted input images, done by third party server without knowing the user's secret key. The input images are the same satellite images but taken at different time instances.

Observations:

The observations from the practical implementation of this model are made to conclude that the change detection using image differencing technique can be performed in a secured way by the other parties without using user's secret key. The decrypted result image is obtained as if the differencing is done on the plain images.



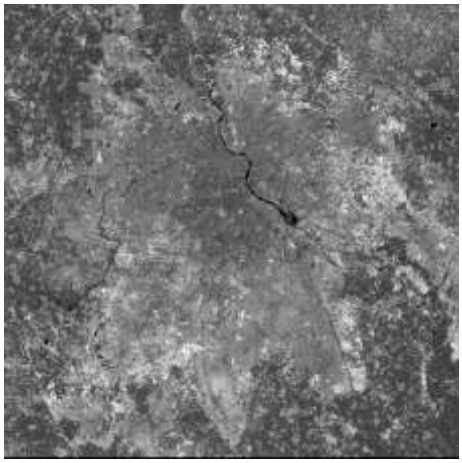
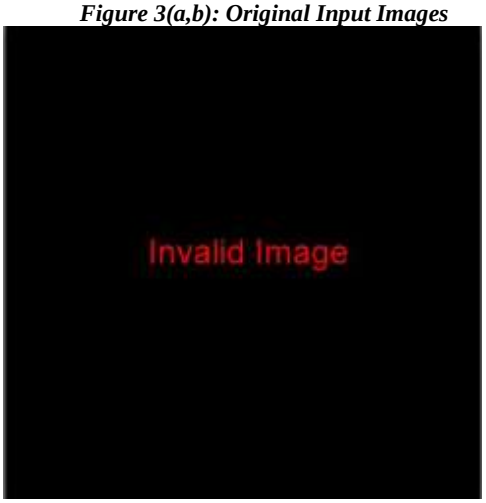


Figure 3(a,b): Original Input Images



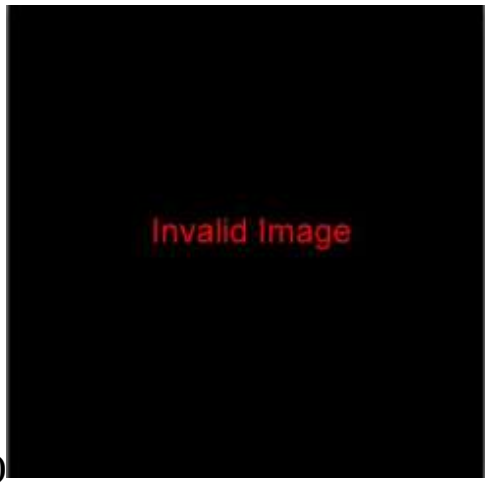


Figure 3(c, d): Encrypted images using Paillier Encryption algorithm

ISSN 2348 – 8034
Impact Factor- 4.022

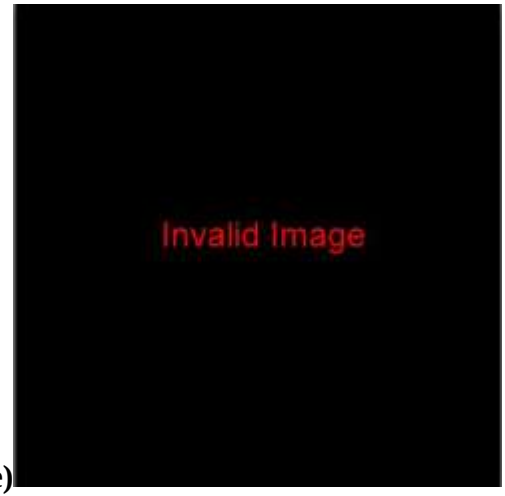
3e) 

Figure (3e): Difference image produced by Homomorphic subtraction

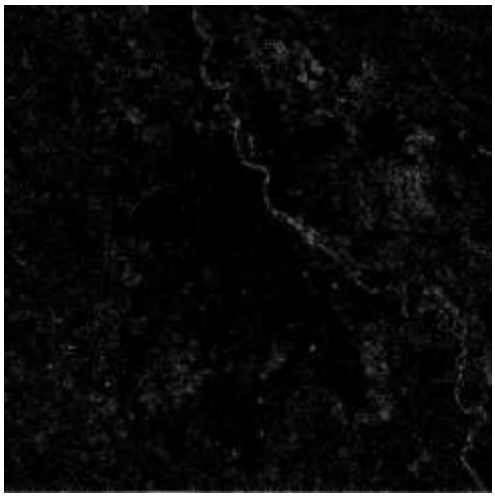
f) 

Figure (3f): Decrypted output Image after applying decryption on the difference image

V. CONCLUSION

In this paper we proposed a framework for the secured change detection of satellite images by adapting the Homomorphic property of the Paillier cryptosystem. The practical implementation of the proposed model is successfully done. Experimental results proved that the pixelwise image differencing operation is possible on the encrypted images that preserves privacy and protects the confidentiality for satellite images with the complete control of the user. Future work will entail two aspects. The other unsupervised change detection techniques can be used to further improve the remote sensing process. The second aspect may be to explore the properties of the somewhat and fully Homomorphic encryption systems for the satellite images.

References

[1] A. Asmat, "The Role Of Remote Sensing In Fighting Against Terrorism- A Case Of Pakistan", Technical Commission VII Symposium ISPRS, Vienna, Austria, 2010.

[2] Chao-Yung Hsu, Chun-Shien Lu, and Soo-Chang Pei , "Image Feature Extraction in Encrypted Domain with Privacy-Preserving SIFT", IEEE Transactions On Image Processing, Vol. 21, November 2012.

[3] Craig Gentry, A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009. crypto.stanford.edu/craig.

[4] Feng Zhao, Chao Li, Chung Feng Liu, "A Cloud Computing Security Solution on Fully Homomorphic Encryption", International Conference on Advanced Communication Technology ICACT, Feb 2014.

[5] Juan Ramon Troncoso-Pastoriza, Daniel Gonzalez-Jimenez, and Fernando Perez-Gonzalez, "Fully Private Noninteractive Face Verification", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 7, July 2013

[6] Krishna Kant Singh, Neelima Saini, Nitin Garg, Sunita Mandal, Nitigya Grover, "Unsupervised Change Detection for Satellite Images using Normalized Neighborhood Ratio and Gustafson KesselClustering", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2013.

[7] Masroor Hussain, DongmeiChen, AngelaCheng, HuiWei, DavidStanley, "Change detection from remotely sensed images: From pixel-based to object-based approaches", ISPRS Journal of Photogrammetry and Remote Sensing 80 (2013), pp. 91–106

[8] Naveed Islam, William Puech and Robert Brouzet, "A Homomorphic Method for sharing secret images" in International Workshop on Digital Watermarking IWDW, Sep2009.

[9] Payal V.Parmar et al., "Survey of Various Homomorphic Encryption Algorithms and Schemes" in International Journal of Computer Applications, April 2014.

[10] Pedro Silveira Pisa, Michel Abdallay, and Otto Carlos Muniz Bandeira Duarte, "Somewhat Homomorphic Encryption Scheme for Arithmetic Operations on Large Integers",

ISSN 2348 – 8034
Impact Factor- 4.022

Global Information Infrastructure and Networking Symposium GIIS, Dec 2012.

[11] Peijia Zheng and Jiwu Huang, "Discrete Wavelet Transform and Data Expansion Reduction in Homomorphic Encrypted Domain", IEEE Transactions on Image Processing, Vol 22, No.6, June 2013.

[12] Photograph courtesy of the U.S. Geological Survey Credit: U.S. Geological Survey, USGS LRS Image Gallery. The USGS home page is http://www.usgs.gov. Web site: http:// remotesensing.usgs.gov/gallery/Remote Sensing Image Gallery.

[13] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms," in *Foundations of Secure Computation*. Cambridge,MA, USA: MIT Press, 1978, pp. 169–178.

[14] R.Naveena Devi, Dr.G.Wiselin Jiji, "Change Detection Techniques – A Survey", International Journal on Computational Sciences & Applications (IJCSA), 2015.

[15] RatnaKumari Challa, G. VijayaKumari, Sunny B, , "Secure Image processing using LWE Based Homomorphic Encryption", IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015.

[16] Rekha Jadhav, "Advanced Change Detection in Satellite Images using DWT", International Journal of Recent Technology and Engineering (IJRTE), 2014.

[17] S.G. Hoggar, "Mathematics of Digital Imaging", Cambridge University Press, 2006.

[18] Samoud Ali, Cherif Adnen, "RSA Algorithm Implementation for Ciphering Medical Imaging", International Journal of Computer and Electronics Research, Volume 1, Issue 2, August 2012.

[19] Wei Wang et al., "Exploring the Feasibility of Fully Homomorphic Encryption", IEEE Transactions On Computers, Vol. 64, No. 3, March 2015

[20] Yan Zhang et al., "A Secure Image Retrieval Based on Homomorphic encryption for cloud computing", Proceedings of the 19th International Conference on Digital Signal Processing, August 2014.