Efficient and Secure Optimized Homomorphic Encryption (OHE) Securing Sensitive Images Data in the Age of Cloud Computing

Revati Raman Dewangan (✉ revati2004@gmail.com)
Bhilai Institute of Technology Durg (C.G.)

Sunita Soni
Bhilai Institute of Technology Durg (C.G.)

Ashish Misal
National Institute of Technology Raipur

Research Article

Keywords: Improved Image Encryption, RGB Image Encryption, Cryptographic System, Image Encryption, Homomorphic Encryption etc...

Posted Date: October 20th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3460853/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.
Efficient and Secure Optimized Homomorphic Encryption (OHE) Securing Sensitive Images Data in the Age of Cloud Computing

Revati Raman Dewangan1, Sunita Soni2, Ashish Misal3
1 Research Scholar, Department of Computer Science and Engineering, Bhilai Institute of Technology Durg (C.G.), revati2004@gmail.com
2 Department of Computer Science Engineering, Bhilai Institute of Technology Durg(C.G.), sunitasoni74@gmail.com
3 Department of Information Technology, National Institute of Technology Raipur (C.G.), amisal.it@nitrr.ac.in

Corresponding Author Email: revati2004@gmail.com

Abstract

The goal of the project is to create a cutting-edge picture encryption technique that can be used to significantly boost the security of encrypted photographs. Since visible electromagnetic spectrum pictures are a difficulty, we provide an ideal homomorphic image encryption method to address the issue. Therefore, in our encryption phase, the numerical intensity value of a pixel from each channel is represented as the average of smaller pixel intensity sub-values. Therefore, each R, G, and B-channel picture is composed of a number of separate photographs. using an encryption key and aOptimized Homomorphic Encryption method, intensity of every pixel sub-value in every component picture is individually encrypted to provide a distributed picture encryption solution. Before being moved or stored, each encrypted component picture may be compressed. Before beginning the decryption process, each encrypted component picture is first, if required, decompressed. The homomorphic characteristic of the encryption technique is then used to encrypt the total of each encrypted component image's individually encrypted pixel intensity sub-values. To optimise the embedding rate of additional data during the encryption phase, six surrounding pixels are combined as a set, creating a novel method. Then, each channel image's original pixel intensities are restored, and extraneous data is removed from the total data. The intensity value for each channel's pixel in this kind of RGB image encryption and decryption, which is likewise created and simulated using software, is represented as the sum of merely two sub-values. The produced cypher pictures are subjected to several security evaluations and tests. The outcomes of these experiments showed the stability and resilience of the homomorphic picture encryption method we proposed, which also improved the security of the connected encrypted photos. Photos that utilise our homomorphic image encryption technique and are incredibly safe.

Key Word - Improved Image Encryption, RGB Image Encryption, Cryptographic System, Image Encryption, Homomorphic Encryption etc....
INTRODUCTION

Information security problems are also covered in this study. Image security and cyber security are sometimes used interchangeably. To further improve the security of encrypted photographs, new encryption methods and techniques may be continuously used. As a result, researchers are continually looking for new encryption techniques that may effectively safeguard information and block any unwanted online conduct. Our objective is to provide an unique homomorphic picture encryption system that can be used to encrypt photos before sending them across insecure channels without affecting their content. The encrypted images can then be recovered using a decryption procedure. When photographs are saved on computer servers or in files[9], the encryption strategy should also provide protection. For our suggested homomorphic picture encryption technique, the visible electromagnetic spectrum covers a wide range of application domains, such as private satellite photos, military and industrial images, particular medical images, fingerprint images, and other visible electromagnetic spectrum images from any industry where security breaches, confidentiality, and integrity are required.For many years, academics from academia, business, and other fields have created and published different image encryption algorithms in the literature. One may include chaos-based encryptions among these picture encryption systems because in certain instances, they encrypt an image's pixel intensity value using a series of events or a system of equations that exhibit chaotic behaviour. Numerous academics have suggested the chaos-based strategy [4], [1],[3],[5],[8].It was demonstrated how to use an unpredictable system to encrypt a picture. Each pixel's value of intensity is changed using Chen's chaos system, and its location inside the limited region is changed randomly using the Arnold cat map. A technique for optical encryption based on different fractional Fourier transform (FRFT) levels was presented by [2]. To create an encrypted image, they combined many orders of inverted discrete FRFT with an interpolated image[6]. Provides an elliptic curve cryptosystem that uses image encryption to convert a collection of pixels into a matching cypher image. [7] describes the development of an image encryption system that uses electrocardiography to generate the first encryption key needed to encrypt a plain picture. The image encryption-then-compression (ETC) technique was recommended. The encrypted and compressed images it produces are strongly secured by this algorithm, which operates in the prediction error domain [10], [11].This work suggests a paradigm shift in which a single plain image is divided into a number of component pictures These are then separately encrypted to form a number of component cypher pictures. The original picture is created by combining the decrypted component cipher-images[12].

This study has been done in text base data to secure file or data in cloud platform using fully homomorphic encryption techniques [13]. In this work, computations on encrypted data may be performed without first having to decode it. The computations that lead to the results are saved in encrypted form, and when they are decrypted, the outcomes are exactly the same as if the procedures had been carried out on the unencrypted data. Private cloud computing and storage may be possible using homomorphic encryption. It is now feasible to encrypt data and submit it for processing in a commercial cloud environment.

THEORETICAL BACKGROUND
In addition to flexibility, an effective image cryptosystem must perform well in terms of overall security. These qualities are necessary for image security.

1. The encryption method must be secure in terms of computation.

   It must take an exceedingly lengthy amount of time to break. As a result, privileged photos shouldn't be readable by unauthorized people.

2. To maintain the system's high performance, encryption and decryption should be quick. The encryption and decryption techniques must be easy enough for consumers to perform on a desktop computer.

3. The security measure should be used as widely as feasible. To build a cryptosystem like a commercial product, it must be broadly accepted.

4. The security system must be adaptable.

5. The encrypted picture data shouldn't be expanded.

As network information transfer formats have evolved with information technology, image data has supplanted text as the preferred format. Likewise, picture information theft technology has progressed in tandem with image encryption technology. We must work towards a stronger picture encryption solution in order to stay up with developing information-theft technologies. The ciphertext displays surprising behaviour when a picture is encrypted using chaotic technology, which outperforms conventional methods, greatly lowering the possibility of decryption. Because of this, chaotic technologically driven algorithms for digital picture encryption have recently taken on more significance. The dual logistical chaotic map is used in this work to examine digital photo encryption techniques. The outcomes of the simulated test are examined using the histogram, pixel correlation, information entropy, key space size, key sensitivity, and other metrics. There are two images used: the conventional Lena picture and a real-world image. The statistics show that this study's methodology has a larger effect on security[14].

The electronic picture Using chaotic mapping, chaotic encryption technology will encrypt, protect, and create the matching decryption for the digital picture method. In contrast to the conventional way of employing computer software to generate pseudorandom numbers, chaotic mapping is currently used extensively in digital picture encryption technologies or Methods based on systems that are chaotic. The pseudorandom number series is the same and much more surprising when the same beginning value is used in the data encryption method based on a chaotic system.

The digital image chaotic encryption system can encrypt data using the image pixel set and chaos pseudorandom number sequences, and it can also generate pseudorandom number sequences for use in the decryption process.

**Proposed Optimized Image Cryptographic (Oic) Scheme**

Then think about the related encryption and decryption methods for the following hypothesis.

A 2D array g(i, j) be displaying a picture with M numbers rows and Nnumbers columns, where small i = 12;3;::; The value of M and J = 12;3;::;N, where j belongs the spatial coordinate of every pixel, number of pixel intensity levels(L) which is equal to 256. The data
class of the picture must be 8-bit which is unsigned integer. Each pixel's intensity value falls between \([0; (L-1)] = [0;255]\) as a consequence. Assume that the intensity value \(y\) of each pixel is a part of the finite Galois Field. \(Z_p\) is equal to 0; 1; 2; \(\ldots\) \((p-1)\), with \(p\) being a prime number equal to 257 \((p)\). It was revealed that the intensity value for each pixel in an 8-bit image that falls within the range \([0;255]\) is \(p\) is equal to 257, the prime number that is closest to 255. This might lead to a pixel intensity value of 256, which is beyond the \([0;255]\) range. Redundancy and other considerations make it unlikely that mapping \(y=256\) to \(y=255\) will significantly alter the original image. As a result, if \(y=256\) occurs then \(y=256\). The creation of pictures from various data types, such an unsigned 16-bit integer, may be accomplished using comparable techniques, as should be mentioned.

\[
Z_p = E(y_1)E(y_2)E(y_3): \ldots E(y_k);
\]

\(k\) is a positive integer such that \(1 \leq k \leq L\). Thus, the product of the values of each sub-encryption is the encryption of a total of \(k\) sub-values of pixel intensity, such as \(y_1; y_2; y_3; \ldots ; y_k\).

### Optimized Homomorphic image encryption

Homomorphic encoding function \(E\), \(y\) is value of pixel intensity in the image \(g(i, j)\),

\[
I = 1; 2; 3; \ldots ; M
\]

\[
j = 1; 2; 3; \ldots ; M.
\]

\(N\) is the number of pixels in the rows and columns of the digital picture. As shown, the average of a pixel's \(k\) sub-values of intensity.

\[
y = y_1 + y_2 + y_3 + y_4 \ldots \ldots y_k = \sum_{n=1}^{k} y_n
\]

\(k\) is the number of pixel components, also known as pixel intensity sub-values or component pictures. When there are more pixels in the image than pixel intensity sub-values, or when \(k > y\), extra-special processing is necessary. The original pixel value \(y\) in this instance may be found using the difference \(d = ky\): If you want to use the Optimized Homomorphic Encryption function \(E\) to encrypt a pixel's intensity value, write:

\[
E(y) = E(y_1 + y_2 + y_3 + y_4 \ldots \ldots y_k) = E(\sum_{n=1}^{k} y_n) = \prod_{n=1}^{k} E(y_n)
\]

The last statement of \(E(y)\) in the previous equation has an important meaning. The same or different encryption keys may be used to distribute, parallelize, or process each \(E(y_k)\) in a sequential or parallel manner. The same or separate processors, located at the same or various locations, may compute each \(E(y_k)\). An attacker might not have access to the entire encrypted image since varied \(E(y_k)\) can be kept or sent at multiple times and locations. If separate for each \(E(y_k)\), it might be difficult to decrypt all of the connected component of encrypted pictures without the decryption keys since adversaries who know one set of decryption keys might not also know the other decryption keys. All that is necessary is that the sum of each \(y_k\) equals \(y\); otherwise, each \(y_k\) may be created at random. It's also worth noting that as \(k\) increases, the encrypted image becomes more secure, but at a larger computational cost. The range of the pixel intensity values for the linked picture is \([0; (L-1)]\), however each encrypted value \(E(y_k)\) may potentially be a very large integer. In order to get the pixel intensity values that are important from the viewpoint of an image and lie between \([0; (p-1)]\), Each of the
encrypted values $E(y_k)$ may be converted back to $Z_p$ by applying \((\mod p)\) to them. For example, the \([0;255]\) pixel intensity range for an 8-bit image allows for the possibility of changing $p$ that is equal to 257. Consequently, we might write:

$$C_1 = E(y_1)$$
$$C_2 = E(y_2)$$
$$\ldots$$
$$C_k = E(y_k)$$

Using the aforementioned equations and \(\mod p\), we have

$$C_{p1} = C_1 \mod p = E(y_1) \mod p$$
$$C_{p2} = C_2 \mod p = E(y_2) \mod p$$
$$\ldots$$
$$C_{pk} = C_k \mod p = E(y_k) \mod p$$

The sub-values of each pixel's intensity, denoted by the letters $C_{p1}$, $C_{p2}$, \ldots s, and $C_{pk}$, are encrypted values. They also represent the intensity sub-values of the secure image pixels that will be sent or preserved. Another quantity that is necessary for the decryption must be specified, which is likewise critical. It is also known as the largest integer, the \((E(y_k)/p)\) floor, or any integer that is smaller than or equal to \((E(y_k)/p)\). Additionally, it shows the result of dividing $E(y_k)$ by $p$. It is not a secret variable, but in order to increase security, it may be computed or sent at the receiver side and encrypted in a variety of methods. It may be difficult to reconstruct $E(y_k)$ for receiver-side decryption applications without $b(E(y_k)=pc$. As a result, we may write:

$$q_{t1} = [(E(y_1)/p]$$
$$q_{t2} = [(E(y_2)/p]$$
$$\ldots$$
$$q_{tk} = [(E(y_k)/p]$$

**Homomorphic Image Decryption Phase**

Allow $C_{p1} = E(y_1) \MOD p$, $C_{p2} = E(y_2) \MOD p$, $C_{p3} = E(y_3) \MOD p$, and typically $C_{pk} = E(y_k) \mod p$ to each of these parameters is assigned a unique encrypted pixel intensity sub-value. \(E\) is a\(\text{Optimized Homomorphic Encryption function on the receiver side of } Z_p\). Allow the receiver side to access the decryption parameters $q_{t1} = (E(y_1)=p), q_{t2} = (E(y_2)=p, q_{t3} = (E(y_3)=p, \ldots q_{tk} = (E(y_k)=p)$.\n
$E(y_1), E(y_2), E(y_3), \ldots$ and $E(y_k)$:

$$E(y_1) = q_{t1} \cdot p + C_{p1}$$
$$E(y_2) = q_{t2} \cdot p + C_{p2}$$
$E(y_k) = q_t X p + C_p$

When there is a distinct integer constant, $q_t$, for each value of $k$, and $p$, plus $C_p$. Following the identification of the aforementioned variables, the following product may be decrypted using the appropriate decryption function $D$ to get the $y$ value.

Calculate the product first.

$$E(y) = \text{product of } \left[ E(y_1), E(y_2), E(y_3), \ldots \ldots, E(y_k) \right]$$

the decryption function yields results after application:

$$D[E(y)] = D[E(y_1) X E(y_2) X E(y_3) \ldots \ldots X E(y_k)]$$

$$D[E(y)] = \prod_{n=1}^{k} E(y_n)$$

$$D[E(y)] = D[E(\sum_{n=1}^{k} y_n)]$$

$$D[E(y)] = D[E(y_1 + y_2 + y_3 + \ldots + y_k)]$$

$$D[E(y)] = y_1 + y_2 + y_3 + \ldots + y_k$$

$$D[E(y)] = y$$

**Methodology For Image Encryption And Decryption**

The block design for the special case implementation is shown when there are two intensity sub-values for each pixel, as seen in Figure 1. Depending on the value of $k$, the homomorphic encryption process block for component pictures in Figure may be enlarged to 3 onwards till 6, or more, producing more encrypted component photos and a better degree of security.
The purpose of the performance and security assessments is to confirm that the proposed homomorphic picture encryption system satisfies certain performance requirements and can fend off security intrusions. Correlograms, information entropy, cypher cycles, histograms, chosen-plaintext assaults, and brute force attacks are all included in these performance and security evaluations. We developed and put to use a laptop with a CPU that met the criteria listed below: Core(TM)Intel (R) i3-1005G1 CPU 1.20 GHz or 1.19 GHz with 8GB of RAM.

**Results Of Analysis And Tests**

A strong encryption system must be able to withstand brute-force attacks, well-known plaintext attacks, ciphertext-only attacks, statistical attacks, differential attacks, and any other known attack. [15-16] For digital pictures, the proposed optimised homomorphic image cryptosystem is assessed for its resilience to statistical, differential, and brute-force assaults [20,24]. The suggested homomorphic picture cryptosystem's security from a strongly cryptographic perspective will be demonstrated. The outcomes demonstrate the suggested cryptosystem's adequate security. Some security analysis findings, including those from critical spatial, statistical, and differential analyses, are provided here[17] Lija's image is put to the test in figure 2.
Information Entropy Analysis

Shannon created a communication and archiving system in 1949 [18] Modern information theory encompasses a wide range of topics, such as error correction, data compression, encryption, and communication networks.

We may compute the entropy $H_m$ of a source, where $m$ uses the equation below:

$$H(m)= \sum_{i=0}^{2^N} p(mi) \log_2 \frac{1}{p(mi)} \text{ bits}$$

$p(mi)$ stands for the likelihood that the sign $mi$ will occur. Bits are used to represent entropy. We investigate it and discover that the entropy of the equation, which is identical to a uniform random source, is $H(m)=8$. A real-world information source's entropy value is often lower than the ideal value since it seldom generates random signals in practise. However, the optimal entropy for encrypted communications should be 8. The security of such a cypher is jeopardised to some extent if it creates symbols with an entropy of eight.

Statistical Analysis

Shannon [18]in that "Many types of cyphers can be solved by statistical analysis." The suggested homomorphic picture cryptosystem is statistically analysed in this study, with a focus on its outstanding confusion and diffusion features, which are particularly resilient to statistical assaults. To demonstrate this, a test was carried out using the histograms of the encrypted photos and the correlation coefficients between pixels in the same place in the plain and cipher images.

Histograms of encrypted images
Figures provide a typical example of the histogram test shown in figure 3-5, where it is possible to observe the histogram of the encrypted picture cypher image generated by the homomorphic cryptosystem. According to Fig. 3, applying a very homogeneous and distinct picture from the initial plain image. With regard to the homomorphic cryptosystem in Fig. 4 displays the outcome. It is obvious that the histogram differs from that generated using the encryption procedure, the results of which are displayed in Figure 5.

Figure 3 Histogram of a Grayscale Image of lija.

Figure 4 (a) original image of lija.jpg, (b) Encrypted Image of lija.jpg and (c) Decrypted image of lija.jpg
Comparison of the plain and cypher pictures' correlation between pixels in the same area

The encryption strength of any image cryptosystem may be ascertained by comparing the correlation coefficient between pixels at the same location in plain and cypher photos [19].

\[ \text{Co}(x,y) = \frac{\text{E}[x - E(x)] \cdot [y - E(y)]}{\text{D}(x)^{1/2} \cdot \text{D}(y)^{1/2}} \]

Further, when \( x \) and \( y \) are the grayscale values of two identical pixels in the plain and cypher images, \( r_{xy} \) is equal to \( \text{co}(x,y)/\text{D}(x)^{1/2}\text{D}(y)^{1/2} \).

Table 1 Correlation coefficient between adjacent pixels in plain and cypher pictures.

<table>
<thead>
<tr>
<th>Encryption algorithm</th>
<th>Correlation coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain Image</td>
<td>0.0042</td>
</tr>
</tbody>
</table>
Homomorphic System | 0.0034

**Key Space Analysis**

Effective picture encryption requires an algorithm that takes into account the cypher keys. Below is a summary of the key space analysis and test results for the proposed homomorphic picture cryptosystem.

A secure image cryptosystem needs a large enough key space to fend off brute force assaults [20]. The RC6 method employs a 128-bit encryption scheme and a key space with a size of 0 to 2040 bits. The number of operations required for a comprehensive key search is k, where k is the key size in bits. The attacker will check every key systematically, at random. Assume the secret key is 128 bits long. It will thus need an adversary $2^{128}$ operations to successfully decode the key. The following calculations are required if the adversary guesses the key using a 1000-MIPS computer:

$$2^{128} \div (1000^6 \times 60 \times 60 \times 24 \times 365) > 11 \times 10^{21} \text{ years}$$

And this is practically not possible.

**Key sensitivity test**

Secure image cryptosystems require large key sensitivity. This indicates that even a small variation between the two cannot be used to properly decrypt the cypher picture. keys for encryption and decryption [21]. Assume that the ciphering key is 16 characters long[22]. This indicates that the key has 128 bits. We do the following actions to evaluate the suggested homomorphic encryption's key sensitivity using the RC6 algorithm:

1. Encrypted image A is the name given to an image that has been created using a secret key consisting of 32 hexadecimal zeros (see Fig. 7 a).

2. By slightly altering the secret key—which is represented by the hexadecimal digits eight and 31 zeros—the exact same picture may be encrypted. The secret key's most crucial digit is changed. Fig. 7 b displays the finished image, sometimes referred to as encrypted image B.

3. The identical picture is encrypted again with a little change to the secret key, which consists of 31 zeroes and one hexadecimal integer. The adjustment is applied to the secret key's least significant digit. The final picture's name is Encrypted image C; see Fig. 7c.
Figure 7: The homomorphic algorithm cryptosystem was tested for key sensitivity using the encrypted picture.

a. A having a 32-digit key.

b. Image B was encrypted using an 8 and 31 zero key.

c. A image encoded using a 31-digit key.

Table 2: Key sensitivities test results of homomorphic algorithm cryptosystem

<table>
<thead>
<tr>
<th>Image 1</th>
<th>Image 2</th>
<th>Correlation Coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>EI of A</td>
<td>EI of B</td>
<td>0.98</td>
</tr>
<tr>
<td>EI of B</td>
<td>EI of C</td>
<td>0.85</td>
</tr>
<tr>
<td>EI of C</td>
<td>EI of A</td>
<td>0.90</td>
</tr>
</tbody>
</table>

Note: Encrypted Image

**Noise's Influence**

This section looks at how noise affects the homomorphic image cryptosystem. The test results demonstrate just how vulnerable to noise the RC6 technique and homomorphic cryptosystem algorithm are. As a consequence, they are appropriate for a tranquil setting. the variation in peak signal-to-noise ratio (PSNR) between the encrypted and unencrypted images for all encryption methods. The performance of the suggested homomorphic cryptosystem is adversely affected by noise. NPCR is 0.35, RC6 is 99.09, and the chaotic baker yields around 100 outcomes using the homomorphic technique.

**Conclusion**

An analysis and an improved homomorphic image cryptosystem are suggested after the study of a number of tests. The results of a security analysis experiment show the significance of such a visual cryptosystem for studying the trade-off between attack cost and information value as well as other properties like operating speed, processing cost, and implementation simplicity. This method provides numerous levels of security since it uses homomorphic domain encryption and watermarks the reflectance component of the picture using the lighting component. Thanks to the strong diffusion mechanism of the system, a little change in the plain picture may result in a large change in the cypher image. The homomorphic cryptosystem approach is better in a noisy environment. In order to safeguard the patient's privacy preservation area, we want to utilise optimal homographic image encryption in the future.

**Declarations**
Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Funding

No external funding is attached to this study.

Availability of data and materials

Data will be provided on request.

Conflict of Interest: The authors don’t have any conflict of interest among them.

References


