Comparative study on satellite based image encryption methods: a survey

Chethana Vasudevaiah[1], Rashmi Shivaswamy[2]
[1]Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Visvesveraya Technological University, Belagavi, India
[2]Department of Computer Science and Engineering (Data Science), Dayananda Sagar College of Engineering, Visvesveraya Technological University, Belagavi, India

Article Info

Article history:

Received Aug 17, 2023
Revised Dec 21, 2023
Accepted Jan 23, 2024

Keywords:

Advanced encryption standard
Encryption
Field programmable gate arrays
Onboard processing
Satellite images

ABSTRACT

The availability of high-resolution satellite images increases with advancements in remote sensing technology. These satellite images are used in various earth observation applications such as disaster management, military applications, weather forecasting, land use and cover, and many more. Satellite images have large volumes stored in memory devices. These satellite images are transmitted to the ground station for processing and analysis. In these cases, images are vulnerable to privacy issues. As technology advances, onboard processing of satellite images using intelligent systems processes the images faster. A model such as field programmable gate arrays (FPGA) is used in onboard processing to process satellite images. However, images are susceptible to faults induced by harsh radiation environments in space. Encryption is one of the most assured methods to provide privacy to satellite images. Hence, encryption of satellite images during processing, storage, and transmission is the present rising demand. There are various encryption methods implemented using algorithms such as advanced encryption standard (AES), homomorphic, advanced encryption standard-counter (AES-CTR), and chaotic maps. Concurrent processing and encryption of images using MapReduce with Hadoop Framework perform the task faster. The focus of this paper is a comparative study of the various encryption methods used in recent years.

Corresponding Author:

Chethana Vasudevaiah
Department of Information Science and Engineering, Dayananda Sagar College of Engineering,
Visvesveraya Technological University
Belagavi-590018, Karnataka, India
Email: chethanav499@gmail.com

1. INTRODUCTION

In India, remote sensing plays a vital role due to monsoons and frequent climate changes leading to natural disasters. Using remote sensing, images are acquired from a distance which covers a large picture of the earth. These pictured images are mainly useful for earth observation applications. The number of satellites launched from various countries is increasing day by day. The Indian Space Research Organization (ISRO) has launched satellites such as Sentinel, CartoSAT, RISAT, INSAT, IMS, IRS, OceanSAT, and many more. In recent years, along with the government, even private sectors also launched satellites known as the agile space sector. Developing countries have the potential to launch satellites to open up space activity in a wider range which is useful for business applications [1]. The satellites can be either traditional satellites or small satellites. Examples of small satellites are nanosatellites, microsatellites, picosatellites, and

CubeSats. The resolution of the small satellite images is very low. Hence, there is a need to enhance the resolution of satellite images. Various methods such as interpolation, pansharpening, deep learning, and many other methods [2] can be used for the above-mentioned purpose. The launching cost and time for traditional satellites are very high when compared to small satellites. These satellites capture large volumes of images and are used for various purposes. Processing and analysis of these images are useful for many applications such as the prediction of landslides, forest fires, rescue operations on post-disaster, post-disaster damage assessment, land use and land cover (LULC) classification, and many more [3]–[9]. With the advancement in space technology small satellites such as CubeSats, nanosatellites, and miniature satellites are launched which are less costly, less power consumable, and easy to manufacture with less weight and less time. Onboard processing of these small satellite images in real time provides faster-analyzed results. These results were mainly used in emergency decision-making, rescue operations, spatial resolution enhancement [10], and military applications such as ship detection [11]. The onboard real-time processing system becomes the brain of intelligent remote-sensing satellites [12]. Real-time processing using graphical processing units (GPU) processes the images with high performance and low power consumption [13]. The increase of small satellites such as CubeSats increases vulnerability to privacy issues. CubeSats which consist of many small satellites acquire large dimensional images that cover large space of earth. The transmission of images between satellite to satellite, and satellite to ground station is more vulnerable to threats. In these cases, providing confidentiality, authenticity, security, privacy, and integrity of satellite image data have become vital issues [14]. Onboard processing of images and transmission of information in real-time also leads to privacy issues [12].

Providing privacy to satellite images using encryption methods is a very challenging task. Encryption of satellite images to get ciphertext and decryption to get original image known as cryptography. There are three types of encryption methods based on their encryption principle. They are symmetric, asymmetric, and hash encryption algorithms. Symmetric encryption algorithms mainly include data encryption standard (DES), triple data encryption standard (3DES), and advanced encryption standard (AES). Asymmetric encryption algorithms mainly include the Rivest Shamir Adleman (RSA) algorithm, digital signature algorithm (DSA), and the elliptic curves cryptography (ECC) algorithm. Hash encryption algorithms mainly include the secure hash algorithm-1 (SHA-1), and message-digest algorithm (MD5) [15]. In the symmetric approach, for both encryption and decryption only one key known as the public key. In the asymmetric approach, two keys: the public key for encryption and private key for decryption are used [16]. Many encryption algorithms such as AES [17]–[19], DES [20], 3-DES [21], Combination of AES, DES, 3-DES algorithm [22], exclusive-or (XOR) keys [23], homomorphic encryption [24], advanced encryption standard-counter (AES-CTR) [25], encryption using deep learning (DL) [26], error detection using hamming code [27] and chaotic encryption [28]–[37] are used to encrypt satellite images. In some cases, combination of two or more encryption algorithms provides more efficient encryption results.

The implementation of encryption algorithms on satellite images takes place on the field programmable gate arrays (FPGA) model. The FPGA model is high in performance, less in cost, suitable for small satellites, and takes less manufacturing time. The FPGA model consists of complex digital circuits that provide faster processing of satellite images even in harsh radiation environments in satellites. In recent days, onboard processing of satellite images is being used on FPGA-based hardware core devices. Onboard processing of complex problems with low energy consumption improves efficiency, accuracy, and performance [38]. Implementation of convolution neural network (CNN) on FPGAs for onboard processing of high-resolution satellite images requires less computational power and low memory resources [39]. The artificial neural network (ANN) model implemented on FPGA can also be used to extract the features from an input image and to encrypt the same image using asymmetric encryption algorithms [40]. Nowadays onboard processing using FPGA model is used in many remote sensing missions such as automatic target detection [41] and ship detection [42]. In onboard processing, the images are induced with some errors due to single-induced upsets. So, providing privacy for satellites is a must in onboard processing using FPGA Hardware [14].

2. LITERATURE REVIEW

According to Al-Khasawneh *et al.* [22], encrypting and decrypting satellite images can be done in the form of batches using a chain-based strategy in real-time. This method provides security to images without compromising any type of attack. For optimal performance, the method combines three encryption algorithms: triple DES, DES, and AES in a chaotic-enhanced MapReduce approach. The MapReduce method is utilized to process the large image sizes that are stored in the Hadoop distributed file system (HDFS). Mapper divides the images into chunks and each chunk consists of a separate key/value (filename, image) pair as per user-provided width and height. The secret key and XOR matrix are generated for encryption. The reducer reduces all the chunk images that are encrypted and merges them into a single image. Each chunk of the image is processed by different nodes in parallel which increases the cost of execution. In this approach, the performance of each system depends on computation speed, external power supply, and total number of systems provided for computation. Cost inflation is proportional to the number of processors. There may exist some outlier nodes that are needed to identify and task to be handed over by another high computational node by using proper job trackers or outlier detectors.

Wibisono *et al.* [23] proposed encryption of satellite images of size M×N using an encryption key by applying exclusive-or (XOR) to get ciphertext. Similarly, decryption is used to get the original image back. In this proposed method, reduces the number of bit errors extracted during decryption. In this way visual quality of the restored satellite images are increased. And also strengthen the security of remote sensing satellite images which are distributed via the internet. Data security techniques such as encryption and reversible data hiding in encryption images (RDHEI), are applied to secure the use of images by unauthorized users. The proposed method only considered red, green, and blue channels of colored satellite images. However, additional data from the images also needs to be considered to correct the errors in the restored satellite images.

Vaseghi *et al.* [43] proposed a chaotic oscillator that provides three chaotic signals. Each signal with 15-digit float values generated from a satellite downlink transmitter. Chaotic keys are generated from chaotic sequences. A suitable master-slave system for encrypting and sending encrypted images is proposed. The original satellite image stream is converted from serial to parallel data and sent to the quadratic amplitude modulation (QAM) mapper. QAM maps the data to constellation points and QAM symbols. These symbols are sends to chaotic constellation for encryption. Multishift cipher algorithm is used for encryption using chaotic keys. Similarly, at ground satellite receiver decryption occurs using the same chaotic keys.

Zhu *et al.* [24] proposed blockchain-empowered privacy-preserving federated learning (PPFL) which uses a homomorphic encryption algorithm during satellite image classification. Federative learning (FL) is a machine learning-based approach to collaborative learning. Images carried with sensitive data are taken in space by satellites. After training a local model with these images for a particular use, the satellite encrypts the data with a homomorphic encryption algorithm and sends it to the edge server. These encrypted local models are gathered by edge servers, who then aggregate and send them to the global satellite model for decryption. Lastly, the edge servers use the decrypted global model to carry out particular tasks. In the homomorphic encryption method trusted authority (TA) uses a key generate function to generate keys for encryption and decryption such as public key (pk) and private key (SK). Using these keys input images are encrypted and decrypted to get ciphertext and plaintext simultaneously. This method mainly minimizes the poison attack without compromising privacy issues. The proposed method uses the blockchain method in which uploading data requires time and gas. With this, efficiency will be reduced which is a very important issue that needs to be considered.

Makhloufi *et al.* [14], [44] proposed cryptography in onboard satellite image processing implementation using FPGA hardware. FPGA mainly supports resource constraint, design flexibility, less cost, less time for manufacture, reliability even in a high radiation environment, more versatile and remotely configurable. Here AES is the algorithm suitable for providing cryptography for images in small satellites. The land surface temperature-split window (LST-SW) algorithm is implemented on FPGA and provides encryption using the AES algorithm for characterizing the land surface with the provided surface temperature derived from thermal infrared window channels using the empirical method.

Alkhelaiwi *et al.* [45] proposed a privacy-preserving deep learning (PPDL) method that uses partially homomorphic encryption (PHE) or Paillier schemes during satellite image classification. This method can be applied in the deep learning-based CNN model and also existing transfer learning models for preserving privacy. This encryption technique uses a single, unbounded range of mathematical operations, such as addition or multiplication. On the side of the client, encryption takes place using partially homomorphic encryption method. For encryption public key is used and it is impossible to decrypt on the server side without knowing the private key. Hence deep learning CNN-based model runs on encrypted input images. More than one PPDL approach can combined to further enhance in efficiency, accuracy in privacy, and classification of satellite images.

Bensikaddour *et al.* [25] proposed a modified AES-CTR along with a Geffe generator to encrypt satellite images with optimized use of resources. AES-CTR is a completely symmetrical and more efficient method for high-performing applications [46]. And also proposed Fridrich's scheme to encrypt multispectral images using chaos-based image encryption that adopts confusion and diffusion methods by changing the positions of the pixels [47].

Ghaleb *et al.* [48] proposed elliptic curve cryptography (ECC) with Diffie-Hellman for satellite image encryption and decryption. Al-Khasawneh *et al.* [49] proposed an enhanced chaotic image encryption algorithm. In this method generated secret key matrices are used to encrypt divided remote sensing satellite image blocks as R, G, and B channels. Encryption is done by XOR operation on an image R with chaos key matrix and exchange recombination. This is repeated for both image G and image B. Now merge the R, G, and B images to get the final encrypted image. The chaotic color image encryption consists of three aspects such as chaos, image, and encryption.

Naim *et al.* [50] proposed a novel approach of an encryption algorithm based on the linear feedback shift register (LFSR) generator, secure hash algorithms-512 (SHA-512) hash function, hyperchaotic systems, and Josephus problem. There is less time complexity and a high level of security with this method. The method provides more security against brute force attacks. Hyperchaotic systems needs more time for preprocessing hence, need to focus on reduction of computation time in future work.

3. METHOD

This paper presents different methods used to encrypt satellite images to provide privacy protections. Each method described with which encryption algorithm used for satellite image encryption. Diagrams are also used for explanation of some encryption processes. The various methods are described as follows:

3.1. Encryption using advanced encryption standard process

The advanced encryption standard (AES) algorithm is a symmetric encryption algorithm using keys of 128, 192 and 256 bits for AES-128 [23], AES-192, and AES-256 [51] block cipher respectively. Input plaintext data is 128 bits (16 Bytes) represented as a 4×4 column-major matrix. The algorithm consists of n iterative rounds and here n depends on key length. If key lengths are 128, 192 or 256 bits then the number of rounds are 10, 12, and 14 respectively [21]. The AES algorithm consists of three stages consists of initial rounds, rounds, and final rounds as shown in Figure 1. In these rounds, transformation such as *SubBytes* transformation, *ShiftRows* transformation, *MixColumns* transformation, and *AddRoundKey* transformation is performed to get cipher data [14], [44]. In between all the rounds, the transformation results are represented as states in the form of a 4×4 column-major matrix. The AES algorithm is described in the following steps:

a. Key expansions: In this step, rounds are generated using a cipher key with lengths 128, 192 or 256 bits used to generate round keys. The discretized skew tent method [52] or Rijndael's keys schedule method [44] used for key generation.

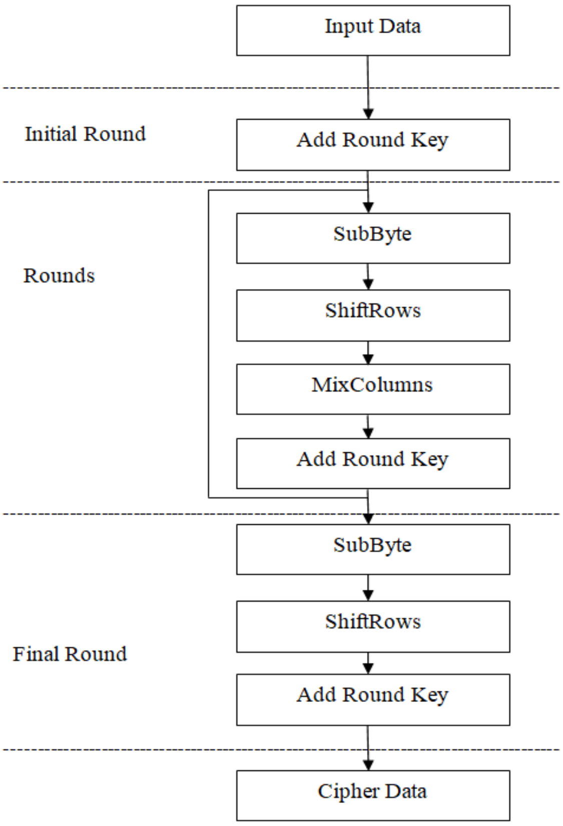

Figure 1. AES encryption process

b. Initial round: It contains *AddRoundKey* transformation in which each byte of input data defined as the state is XOR with a round key to get the initial round intermediate state.
c. Rounds: There are N numbers of rounds are considered based on key length. All these rounds consist of *SubByte, ShiftRows, MixColumns,* and *AddRoundKey* transformations as described below.
d. *SubByte* transformation: In this transformation, each byte of the state matrix of the input image is replaced by an element of the substitution table or S-box which is a predefined 16×16 matrix. The S-box is formed of a lookup table of size 256 bytes. This transformation results in an intermediate state as input for the next transformation.
e. The *ShiftRows* transformation: In this transformation, shift the rows of state by performing one left shift. The first row remains as it is, and the remaining rows 1, 2, and 3 shift left cyclically by one byte, two bytes, and three bytes respectively [44], resulting in a new state.
f. *MixColumns* transformation: In this transformation, each column is considered independently and multiplied by some fixed matrix consisting of three values. Multiply with the first value, no change occurs. Multiply with the second value one left shift has taken place. Multiply with the third value one left shift occurs, immediately XOR this value with before shift state data gives an intermediate state matrix.
g. *AddRoundKey* transformation: In this transformation state of each stage XOR with *RoundKey* to get the intermediate state matrix.
h. Final round: In this, only one round with transformations such as *SubByte, ShiftRows*, and *AddRoundKey*, no *MixColumn* transformation took place. This round results in a final cipher data in the form of a state matrix.

3.2. Encryption using partially homomorphic encryption algorithm in CNN model

Here, satellite image encryption taken place by partially homomorphic encryption (PHE) which described as Paillier scheme [45]. This encrypted satellite images are sent to CNN model for feature extraction and further analysis. More number of satellite images are used for training using CNN model leads to better results. The Paillier scheme encryption consists of key generation, encryption, and decryption algorithms are given below:

Algorithm 1. Key generation (p, q)

```
Input: Generate two unique prime numbers, $a$, and $b$ and confirm that: $gcd(a \times b, (a-1)\ (b-1)) = 1$, where $gcd$ represents the greatest common divisor.
Output: $(pk, sk)$
1.  If $length(p) == length(q)$. Then
2.  Compute $n = p \times q, \lambda = lcm(p-1, q-1)$, where lcm represents the least common multiple.
3.  Choose a random integer $g \in Z^*_{n^2}$ (between 1 and $n^2$)
4.  Define the function: $L(x) = ((x-1)/n)$.
5.  Verify the existence of the following modular multiplicative inverse to ensure that $n$ divides $g$'s order:
    $\mu = L\left(g^{\lambda}\ mod(n^2)\right)^{-1}\ mod(n)$
```

Algorithm 2. Encryption (m, pk)

```
Input: Message to encrypt where $m \in Z_n$
Output: $c \in z_{n^2}$
1.  Choose a random integer $r \in\ Z^*_{n^2}$(between 1 and $n^2$)
2.  Compute the ciphertext as: $c = (g^m \times r^n)\ mod(n^2)$
```

Algorithm 3. Decryption

```
Input: $c \in z_{n^2}$
Output: $m \in z_{n^2}$
1.  Calculate the plaintext message as: $m = L(c^{\lambda}\ mod\ (n^2)) \times \mu\ mod(n)$
```

The public key for encryption is (n, g) and the private key for decryption is (λ, μ).

3.3. Encryption using chaos synchronization approach

In this method, chaos synchronization used for secure satellite image encryption. Master system or chaotic system creates signals such as $x1(t), x2(t)$, and $x3(t)$. The description of these signals [43] are as follows:

$$x1(t) = \alpha(x2(t) - f(x1(t))$$
$$x2(t) = x1(t) - x2(t) + x3(t)$$
$$x3(t) = -\eta\ x2(t)$$

where α and η are nonnegative unvarying parameters.

A Slave system or chaotic system creates signals such as $y1(t), y2(t)$, and $y3(t)$. The description of these signals are as follows:

$$y1(t) = \lambda sgn(x1(t) - y1(t))$$
$$y2(t) = y1(t) - y2(t) + y3(t) + u1(t)$$
$$y3(t) = -(\eta - \Delta\, \eta(t))\, y2(t) + u2(t)$$

where, λ is the design parameter, $\Delta\eta(t)$ is time-varying; Uncertain parameters, $u1(t)$ and $u2(t)$ are two control input signals. Now, using chaotic signals $x1(t), x2(t)$ and $x3(t)$, choatic keys $k1(t), k2(t)$ and $k3(t)$ as follows:

$$k1(t) = mod(x1(t), floor(x1(t-1)))$$
$$k2(t) = mod(x2(t), floor(x2(t-1)))$$
$$k3(t) = mod(x3(t), floor(x3(t-1)))$$

With these keys, encryption takes place using multi-shift cipher algorithm.

3.4. Encryption using MapReduce based approach

Large-sized satellite images are partitioned into several chunks by Mapper and processed in parallel. Then combine the results by reducer to get the final result. Hadoop distributed file system in which distributed systems are used for processing the tasks in parallel to increase efficiency using the Hadoop framework [22]. Hadoop image encryption workflow is shown in Figure 2.

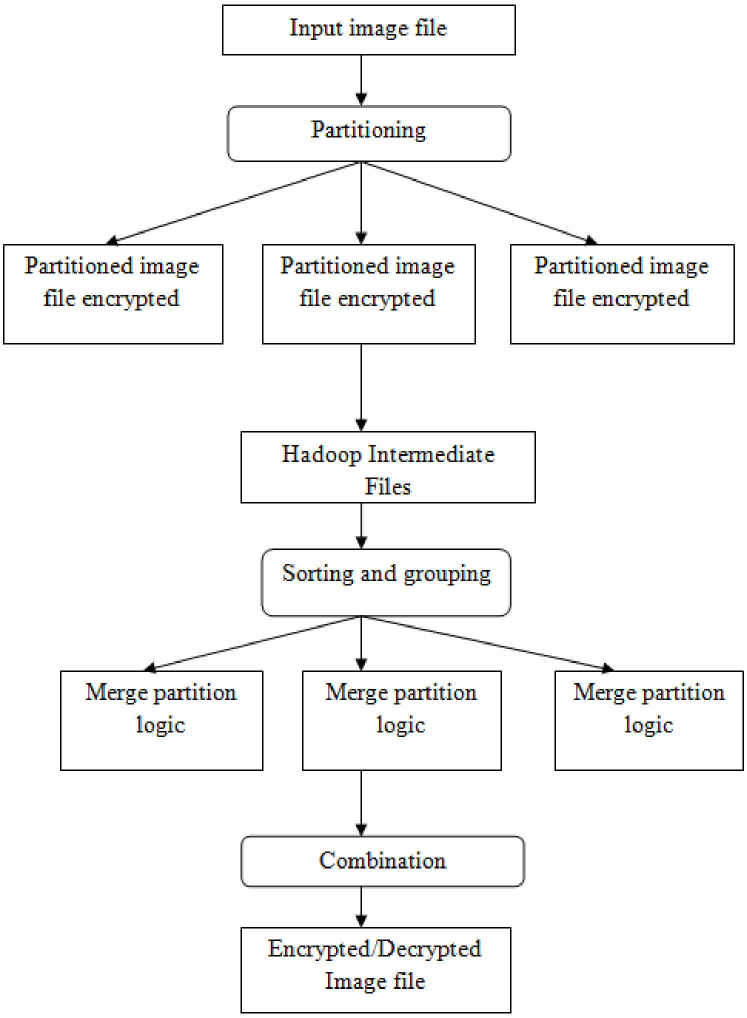
Input image file
Partitioning
Partitioned image file encrypted
Partitioned image file encrypted
Partitioned image file encrypted
Hadoop Intermediate Files
Sorting and grouping
Merge partition logic
Merge partition logic
Merge partition logic
Combination
Encrypted/Decrypted Image file

Figure 2. Hadoop image encryption workflow

The pseudocode of the encryption method is as follows:

a. Input satellite image split into several chunks as per the user-specified height and width. These images are sent to different nodes of the Hadoop framework with key-value pair (filename, image) by Mapper.
b. To encrypt these images at different nodes secret key and XOR matrix are generated.
c. Using these secret keys and the XOR matrix encryption and decryption are taken place.
d. After the encryption or decryption by Mapper, the combined results of Mapper combined at reducer to get the final resultant image.

3.5. Encryption using privacy-preserving federated learning

In this approach of learning local models are trained for any application and later uploaded the trained model and their parameters directly to semi-honest servers for further processes such as aggregation without revealing anything to the third party for privacy protection. Later user receives the global model from this server for any updations. The homomorphic encryption (HE) algorithm is used as it provides more accuracy and strong privacy. The Homomorphic encryption algorithm [24] is described using polytime algorithms (KeyGenerate, Encrypt, Decrypt) as follows:

a. $KeyGeneration(k) \rightarrow EncrptionKey$, Decryption Key (EK, DK). Upon receiving security parameter *k*, the *KeyGeneration* function is used to generate a key pair (EK, DK).
b. $Encryption(PK, s) \rightarrow c$. Encrypting the given input denoted by s using encryption key EK which is a public key to get ciphertext *c* as output.
c. $Decryption(DK, c) \rightarrow s$. Decrypt takes the cipher text data and private key DK as inputs and outputs the corresponding plaintext data as *s*.

Homomorphic encryption consists of two properties additive HE and multiplicative HE [45]. Additive and multiplicative HE equations for given two plaintexts P1 and P2, are as follows:

$$Encryption\ (P1 + P2) = \ Encryption(P1) + Encryption(P2)$$

$$Encryption\ (P1 \times P2) = \ Encryption(P1) \times Encryption(P2)$$

3.6. Encryption using XOR operation on color images

In this method, original satellite image of pixel size is considered.Then, extraction of red, green, and blue channels these color images. Now, image is encrypted using encryption key by applying bitwise exclusive-or (XOR) as shown in Figure 3. Consider *p* to be an 8-bit cover color satellite image of size M×N and each pixel of the image represented as $\mathrm{p_{i,j}}$ located at (i, j) location. Then ciphertext [23] is given by:

$$\mathrm{C_{i,j}} = \sum\nolimits_{\mathrm{l}=0}^{7} \mathrm{C_{i,j}^{l}} \times 2^{\mathrm{l}}$$

where,

$$\mathrm{C_{i,j}^{l}} = \mathrm{p_{i,j}^{l}} \oplus \mathrm{r_{i,j}^{l}},\ l = 0,1, \dots \dots \dots .,7$$

$$\mathrm{p_{i,j}^{l}} = \left\lfloor \frac{\mathrm{p_{i,j}}}{2^{\mathrm{l}}} \right\rfloor \mathrm{mod}2,\ l = 0,1, \dots \dots \dots .,7$$

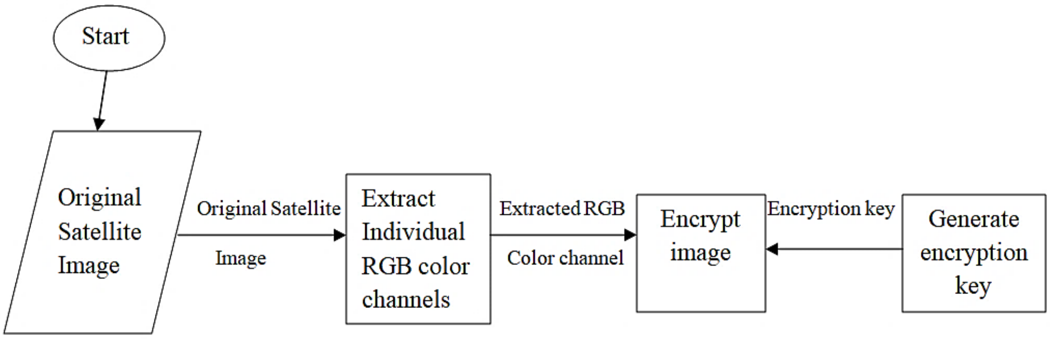

Figure 3. Encryption process

4. RESULT AND DISCUSSION

4.1. Comparative study of various encryption methods

In this section, Table 1 provides a comparative study of various encryption methods. Advantages and the limitations of each encryption methods are listed out in the table. Suggestions for future work are provided in remarks column of the table.

Table 1. Comparative study of various encryption methods

Title of paper/year/reference	Methods used	Advantages	Limitations	Remarks
FPGA/LST-SW encryption module implementation for satellite remote sensing secure systems/2020/[44]	encryption using AES process	Efficient and secure satellite image encryption. And also provides considerable and promising performance.	Hardware errors may lead to inefficient results. If the encryption key changes, then it is very difficult to get the correct correlation coefficient between encrypted and decrypted images.	Other symmetric algorithms can be used along with the AES algorithm.
Finite-time chaos synchronization in time-delay channel and its application to satellite image encryption in orthogonal frequency division multiplexing (OFDM) communication systems/2021/[43]	Satellite image encryption in OFDM communication systems	Easy implementable, low time consumption, secure and reliable approach. High security for statistical attacks	Synchronization time may vary unexpectedly	Traditional and statistical algorithms can be incorporated for encryption/ decryption
An efficient approach based on privacy-preserving deep learning for satellite image classification/2021/[44]	Privacy-preserving deep learning for satellite image classification	Model results with an accuracy of 94.04% for the training, 94.30% for validation, and 90.92% for testing dataset.	Performed encryption operation with only a few datasets	Perform encryption using hybrid privacy preserving deep learning neural technique need to be consider
A MapReduce based approach for secure batch satellite image encryption/2023/[22]	Encryption using MapReduce based approach	Nodes performed with more than 50% efficiency.	Need more processors for enhancing efficiency.	Detecting outlier nodes may increase performance efficiency.
Privacy-preserving federated learning of remote sensing image classification with dishonest majority/2023/[24]	Encryption using privacy-preserving federated learning	An accuracy of 92.5%, if the attack is assumed to be 20% is achieved in the experiments.	Lots of resources and time used. Untargeted attacks reduced efficiency.	Implementation using blockchain with less resources and less gas time needed.
Hybrid reversible data hiding in encrypted satellite images using fluctuation modification extraction and reed-Solomon code embedding/2021/[23]	Encryption using XOR operation on color images	The efficiency of encryption is good.	Considered only red, green, and blue channels from colored image	Other than red, green, and blue channels are need to consider

4.2. Discussion

The survey on various satellite image encryption methods is discussed in this paper. Each discussed encryption methods have its advantages and limitations. As per the study encryption method using the AES encryption algorithm on the FPGA model provides high performance for satellite image encryption. This method shows that onboard processing and encryption of satellite images is efficient in terms of usage of less memory and less time. Need to work on other symmetric encryption algorithms for better results. Another method discussed is a master-slave chaotic system used for encryption. This method combines the multi-shift cipher algorithm with chaotic keys to encrypt satellite images. This method completely removes the appearance of the original satellite image during transmission. However, the method has an unknown time delay. Therefore, some traditional algorithms can be incorporated to control time delay. In recent days, homomorphic encryption combined with deep learning models has produced more accurate outcomes. The observation indicates that hybrid encryption, which combines differential privacy (DP), Secure multi-party computation (SMPC), and secret sharing (SS), may improve the outcome. Accuracy is predicted to rise with larger data sets used for model training. To improve the security of satellite images not only during transmission but also during storage, the MapReduce approach is used. Large datasets of satellite images were encrypted using MapReduce. By detecting outlier nodes in time, efficiency rises as more systems and processors are employed. There are some encryption methods such as homomorphic encryption and the blockchain-powered privacy-preserving federated learning (PPFL) framework needs more time and resources. However, these methods are less effective in untargeted attacks even though yield more accurate results. Finally, the topic of encrypting color satellite images using XOR operations is addressed. The only satellite image channels taken into consideration for encryption are red, green, and blue. To get better results, other color image channels could be taken into consideration.

5. CONCLUSION

This paper provides a review study of various methods and algorithms for encrypting satellite images. First introduced the need for encryption of satellite images and available encryption algorithms. The survey provides theoretical knowledge about various encryption approaches such as AES encryption method, Homomorphic encryption method used in CNN model, XOR encryption used in the Hadoop MapReduce framework, chaos synchronization approach and privacy preserving federated learning method. Based on this study, Encryption of satellite images using privacy-preserving deep learning approach, Hadoop distributed file, and AES methods are found more efficient and recommended for further research in the area of providing privacy to satellite images.

REFERENCES

[1] O. Kodheli *et al.*, "Satellite communications in the new space era: a survey and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, 2021, doi: 10.1109/COMST.2020.3028247.

[2] K. Karwowska and D. Wierzbicki, "Using super-resolution algorithms for small satellite imagery: a systematic review," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 15, pp. 3292–3312, 2022, doi: 10.1109/JSTARS.2022.3167646.

[3] M. Maskey, R. Ramachandran, J. J. Miller, J. Zhang, and I. Gurung, "Earth science deep learning: applications and lessons learned," in *IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium*, Jul. 2018, pp. 1760–1763, doi: 10.1109/IGARSS.2018.8517346.

[4] S. Shakya, S. Kumar, and M. Goswami, "Deep learning algorithm for satellite imaging based cyclone detection," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 13, pp. 827–839, 2020, doi: 10.1109/JSTARS.2020.2970253.

[5] D. Meghanadh, V. K. Maurya, M. Kumar, and R. Dwivedi, "Automatic detection of landslides based on machine learning framework," in *2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS*, Jul. 2021, pp. 8460–8463, doi: 10.1109/IGARSS47720.2021.9553341.

[6] C. Liu, L. Ge, and S. M. E. Sepasgozar, "Post-disaster classification of building damage using transfer learning," in *2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS*, Jul. 2021, pp. 2194–2197, doi: 10.1109/IGARSS47720.2021.9554795.

[7] Z. Deng and G. Zhang, "An improved forest fire monitoring algorithm with three-dimensional otsu," *IEEE Access*, vol. 9, pp. 118367–118378, 2021, doi: 10.1109/ACCESS.2021.3105382.

[8] V. Khryashchev and R. Larionov, "Wildfire segmentation on satellite images using deep learning," in *2020 Moscow Workshop on Electronic and Networking Technologies (MWENT)*, Mar. 2020, pp. 1–5, doi: 10.1109/MWENT47943.2020.9067475.

[9] C. Chen *et al.*, "Dynamic monitoring and analysis of land-use and land-cover change using landsat multitemporal data in the Zhoushan Archipelago, China," *IEEE Access*, vol. 8, pp. 210360–210369, 2020, doi: 10.1109/ACCESS.2020.3036128.

[10] F. Viel, W. D. Parreira, A. A. Susin, and C. A. Zeferino, "A hardware accelerator for onboard spatial resolution enhancement of hyperspectral images," *IEEE Geoscience and Remote Sensing Letters*, vol. 18, no. 10, pp. 1796–1800, Oct. 2021, doi: 10.1109/LGRS.2020.3009019.

[11] A. P. Arechiga, A. J. Michaels, and J. T. Black, "Onboard image processing for small satellites," in *NAECON 2018 - IEEE National Aerospace and Electronics Conference*, Jul. 2018, pp. 234–240, doi: 10.1109/NAECON.2018.8556744.

[12] B. Zhang *et al.*, "Progress and challenges in intelligent remote sensing satellite systems," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 15, pp. 1814–1822, 2022, doi: 10.1109/JSTARS.2022.3148139.

[13] T. Yang, Q. Xu, F. Meng, and S. Zhang, "Distributed real-time image processing of formation flying SAR based on embedded GPUs," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 15, pp. 6495–6505, 2022, doi: 10.1109/JSTARS.2022.3197199.

[14] A. El Makhloufi, N. Tagmouti, N. Chekroun, S. El Adib, J. A. Sobrino, and N. Raissouni, "AES/FPGA encryption module integration for satellite remote sensing systems: LST-SW case," in *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, Sep. 2020, pp. 1–7, doi: 10.1109/CommNet49926.2020.9199644.

[15] C. Wang, Z. Zhang, J. Wu, C. Chen, and F. Gao, "An overview of protected satellite communications in intelligent age," *Science China Information Sciences*, vol. 64, no. 6, Jun. 2021, doi: 10.1007/s11432-019-2928-9.

[16] M. A. Al-Khasawneh, W. Abu-Ulbeh, and A. M. Khasawneh, "Satellite images encryption review," in *2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI)*, Dec. 2020, pp. 121–125, doi: 10.1109/ICHCI51889.2020.00034.

[17] X. Zhang and X. Wang, "Remote-sensing image encryption algorithm using the advanced encryption standard," *Applied Sciences*, vol. 8, no. 9, Sep. 2018, doi: 10.3390/app8091540.

[18] S. Naman, S. Bhattacharyya, and T. Saha, "Remote sensing and advanced encryption standard using 256-Bit key," *Emerging Technology in Modelling and Graphics*, 2020, pp. 181–190, doi: 10.1007/978-981-13-7403-6_18.

[19] H. Lin, X. Xu, M. Bilal, Y. Cheng, and D. Liu, "Intelligent retrieval of radar reflectivity factor with privacy protection under meteorological satellite remote sensing," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 16, pp. 6948–6957, 2023, doi: 10.1109/JSTARS.2023.3296908.

[20] J. D. Gaur, A. Kumar Singh, N. P. Singh, and G. Rajan V, "Comparative study on different encryption and decryption algorithm," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Mar. 2021, pp. 903–908, doi: 10.1109/ICACITE51222.2021.9404734.

[21] S. P. Guruprasad and B. S. Chandrasekar, "An evaluation framework for security algorithms performance realization on FPGA," in *2018 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, Feb. 2018, pp. 1–6, doi: 10.1109/ICCTAC.2018.8370396.

[22] M. A. S. Al-Khasawneh, M. Faheem, E. A. Aldhahri, A. Alzahrani, and A. A. Alarood, "A MapReduce based approach for secure batch satellite image encryption," *IEEE Access*, vol. 11, pp. 62865–62878, 2023, doi: 10.1109/ACCESS.2023.3279719.

[23] G. Wibisono, A. S. Nasution, T. Firmansyah, and A. S. Prabuwono, "Hybrid reversible data hiding in encrypted satellite images using fluctuation modification extraction and reed-Solomon code embedding," *IEEE Access*, vol. 8, pp. 221367–221384, 2020, doi: 10.1109/ACCESS.2020.3042971.

[24] J. Zhu, J. Wu, A. K. Bashir, Q. Pan, and W. Yang, "Privacy-preserving federated learning of remote sensing image classification

with dishonest majority," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 16, pp. 4685–4698, 2023, doi: 10.1109/JSTARS.2023.3276781.

[25] E.-H. Bensikaddour, Y. Bentoutou, and N. Taleb, "Satellite image encryption method based on AES-CTR algorithm and GEFFE generator," in *2017 8th International Conference on Recent Advances in Space Technologies (RAST)*, Jun. 2017, pp. 247–252, doi: 10.1109/RAST.2017.8002953.

[26] K. Panwar, S. Kukreja, A. Singh, and K. K. Singh, "Towards deep learning for efficient image encryption," *Procedia Computer Science*, vol. 218, pp. 644–650, 2023, doi: 10.1016/j.procs.2023.01.046.

[27] A. Patra *et al.*, "Remote sensing image encryption and error detection using hamming code," *Journal of Physics: Conference Series*, vol. 2286, no. 1, Jul. 2022, doi: 10.1088/1742-6596/2286/1/012018.

[28] B. Zolfaghari and T. Koshiba, "Chaotic image encryption: state-of-the-art, ecosystem, and future roadmap," *Applied System Innovation*, vol. 5, no. 3, Jun. 2022, doi: 10.3390/asi5030057.

[29] X. Wang, Y. Zhao, H. Zhang, and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," *Optics and Lasers in Engineering*, vol. 82, pp. 79–86, Jul. 2016, doi: 10.1016/j.optlaseng.2015.12.006.

[30] Z. M. Z. Muhammad and F. Ozkaynak, "ecurity problems of chaotic image encryption algorithms based on cryptanalysis driven design technique," *IEEE Access*, vol. 7, pp. 99945–99953, 2019, doi: 10.1109/ACCESS.2019.2930606.

[31] D. Li, S. Zhou, and C. He, "The application of image encryption method based on chaotic mapping in the field of radar transmitter remote monitor system," in *2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, Oct. 2019, pp. 577–580, doi: 10.1109/IMCEC46724.2019.8983923.

[32] T.-C. Yeh and J.-F. Kiang, "Second-order chaotic maps with random coefficients to generate complex chaotic sequences for high-security image encryption," *IEEE Access*, vol. 11, pp. 83833–83851, 2023, doi: 10.1109/ACCESS.2023.3302012.

[33] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology*, vol. 101, pp. 30–41, May 2018, doi: 10.1016/j.optlastec.2017.10.024.

[34] M. Al Duhayyim *et al.*, "Remote sensing image encryption using optimal key generation-based chaotic encryption," *Computer Systems Science and Engineering*, vol. 46, no. 3, pp. 3209–3223, 2023, doi: 10.32604/csse.2023.034185.

[35] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.

[36] X. Xu and S. Chen, "A remote sensing image encryption method combining chaotic neuron and tent map," *Journal of Computers*, vol. 32, no. 2, pp. 108–123, 2021.

[37] L. Gong, C. Deng, S. Pan, and N. Zhou, "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," *Optics & Laser Technology*, vol. 103, pp. 48–58, Jul. 2018, doi: 10.1016/j.optlastec.2018.01.007.

[38] D. Mota *et al.*, "Onboard processing of synthetic aperture radar backprojection algorithm in FPGA," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 15, pp. 3600–3611, 2022, doi: 10.1109/JSTARS.2022.3169828.

[39] R. Neris, A. Rodriguez, R. Guerra, S. Lopez, and R. Sarmiento, "FPGA-based implementation of a CNN architecture for the on-board processing of very high-resolution remote sensing images," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 15, pp. 3740–3750, 2022, doi: 10.1109/JSTARS.2022.3169330.

[40] Y. Nagasree, C. Rupa, P. Akshitha, G. Srivastava, T. R. Gadekallu, and K. Lakshmanna, "Preserving privacy of classified authentic satellite lane imagery using proxy re-encryption and UAV technologies," *Drones*, vol. 7, no. 1, Jan. 2023, doi: 10.3390/drones7010053.

[41] R. Macias, S. Bernabe, D. Bascones, and C. Gonzalez, "FPGA implementation of a hardware optimized automatic target detection and classification algorithm for hyperspectral image analysis," *IEEE Geoscience and Remote Sensing Letters*, vol. 19, pp. 1–5, 2022, doi: 10.1109/LGRS.2022.3189109.

[42] M. Xu, L. Chen, H. Shi, Z. Yang, J. Li, and T. Long, "FPGA-based implementation of ship detection for satellite on-board processing," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 15, pp. 9733–9745, 2022, doi: 10.1109/JSTARS.2022.3218440.

[43] B. Vaseghi, S. S. Hashemi, S. Mobayen, and A. Fekih, "Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems," *IEEE Access*, vol. 9, pp. 21332–21344, 2021, doi: 10.1109/ACCESS.2021.3055580.

[44] A. El Makhloufi, N. Chekroun, N. Tagmouti, S. El Adib, J. A. Sobrino, and N. Raissouni, "FPGA/LST-SW encryption nodule implementation for satellite remote sensing secure systems," in *2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS)*, Oct. 2020, pp. 1–7, doi: 10.1109/ICDS50568.2020.9268739.

[45] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, and M. Driss, "An efficient approach based on privacy-preserving deep learning for satellite image classification," *Remote Sensing*, vol. 13, no. 11, Jun. 2021, doi: 10.3390/rs13112221.

[46] N. Cherrid, R. Saidi, T. Bentahar, and H. Mayache, "Study of the sensitivity of an InSAR interferogram encrypted by the AES-128 algorithm," in *2021 18th International Multi-Conference on Systems, Signals & Devices (SSD)*, Mar. 2021, pp. 457–462, doi: 10.1109/SSD52085.2021.9429323.

[47] E.-H. Bensikaddour, Y. Bentoutou, and N. Taleb, "Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 1, pp. 50–56, Jan. 2020, doi: 10.1016/j.jksuci.2018.05.002.

[48] A. A. M. Ghaleb, S. Sasi, and A. R. Aswatha, "Design and implementation of satellite image encryption by using ECC," in *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, May 2018, pp. 1438–1443, doi: 10.1109/RTEICT42901.2018.9012322.

[49] M. A. Al-Khasawneh, S. M. Shamsuddin, S. Hasan, and A. A. Bakar, "An improved chaotic image encryption algorithm," in *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Jul. 2018, pp. 1–8, doi: 10.1109/ICSCEE.2018.8538373.

[50] M. Naim, A. Ali Pacha, and C. Serief, "A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem," *Advances in Space Research*, vol. 67, no. 7, pp. 2077–2103, Apr. 2021, doi: 10.1016/j.asr.2021.01.018.

[51] M. Gunasekaran, K. Rahul, and S. Yachareni, "Virtex 7 FPGA implementation of 256 bit key AES algorithm with key schedule and sub bytes block optimization," in *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Apr. 2021, pp. 1–6, doi: 10.1109/IEMTRONICS52119.2021.9422547.

[52] E. Bensikaddour and Y. Bentoutou, "Satellite image encryption based on AES and discretised chaotic maps," *Automatic Control and Computer Sciences*, vol. 54, no. 5, pp. 446–455, Sep. 2020, doi: 10.3103/S014641162005003X.

BIOGRAPHIES OF AUTHORS

Chethana Vasudevaiah received an M.Tech. degree in computer science and engineering from Visvesvaraya Technological University, Belgaum, India. She is currently a research scholar in the Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore. Her research interest includes remote sensing, network security, image processing, artificial intelligence and machine learning. She can be contacted at email: chethanav499@gmail.com.

Rashmi Shivaswamy is currently in charge Head of the Department in Department of Computer Science and Engineering (Data Science) at Dayananda Sagar College of Engineering, Bengaluru. She was previously working as an associate professor, in the Department of Information Science and Engineering at Dayananda Sagar College of Engineering, Bengaluru. She has worked at various engineering colleges such as National Institute of Engineering, Mysore, East Point College of Engineering and Technology, Bengaluru. She also worked in university such as Dayananda Sagar University, Bengaluru. She completed her B.E Graduation in computer science and engineering during 2001 from Mysore University and master's in computer network engineering from National Institute of Engineering. She earned her Ph.D. degree in computer science and engineering from Visvesvaraya Technological University, Belgaum. Her Ph.D. work is in the area of cloud computing. She is an IEEE senior member and has worked as a Managing Committee Member of Computer Society of India, Bangalore chapter for the year 2019-2020. She has served as a Publicity chair for an International Conference on "Applications of Artificial Intelligence and Computational Mathematics-2020". In her credit, she has Book Chapters published by IGI Global. She also presented and published research papers in both National and International Conferences and peer reviewed journals. She has contributed as a reviewer for many Journals. She has guided 2 Projects approved and funded by the Karnataka State Council for Science and Technology (KSCST) under "Student Project Programme-44th Series and 46th Series". She has 2 Indian Patents published. Her main research interests include cloud computing, cyber security, IoT, machine learning and blockchain technology. She can be contacted at email: rashmineha.s@gmail.com.