Remote Sensing and Advanced Encryption Standard Using 256-Bit Key

Sumiran Naman, Sayari Bhattacharyya and Tufan Saha

Abstract The most convenient way of data acquisition in recent times is undoubtedly through remote sensing. Remote sensing data has shown substantial growth in terms of pliability, reliability, cost-effectiveness, speed and efficiency. However, the growth is prone to data breaches and attacks. The commonly employed method for data security is encryption and decryption. This paper proposes the secure transmission of remote sensed data by using AES (Rijndael) algorithm with 256-bit key as the underlying encryption algorithm.

Keywords Remote sensing · Encryption · Decryption · AES-256

1 Introduction

National Remote Sensing Centre (NRSC) defines remote sensing as the most convenient way of data acquisition in recent times [1]. Remote sensing is acquiring information about an object without making any physical contact. Basically, it refers to satellite or aircraft-based sensor technologies for recognition, categorisation and capturing specific details of objects on Earth. Image processing technique is used to extract quantitative information from an image. Remote sensed image processing in recent days has been accounting to a larger space in the current research era. The data sources used in GIS are majorly comprised of remotely sensed data.

Data interception and breach attacks have shown an exponential increase in recent days. The data transmission occurring between the various communication channels

S. Naman · S. Bhattacharyya (✉) · T. Saha
Department of Computer Science and Engineering, Institute of Engineering
and Management, Kolkata, India
e-mail: iamsay253@gmail.com

S. Naman
e-mail: sumiran.naman.rs@gmail.com

T. Saha
e-mail: tufan.saha@outlook.com

J. K. Mandal and D. Bhattacharya (eds.), *Emerging Technology in Modelling and Graphics*, Advances in Intelligent Systems and Computing 937,
https://doi.org/10.1007/978-981-13-7403-6_18

are always vulnerable and the chances of illegal acquisition is directly proportional to the confidentiality attached with the data. The recent actions of satellite interceptions have shown alarming and catastrophic threats pertaining to the national security as well. Here is where encrypting of the data over communication channel becomes an inalienable data characteristic for secure and efficient transmission. The encryption algorithm used here is AES (Advanced Encryption Standard) also referred as Rijndael algorithm. AES algorithm was accepted by the US National Institute of Standards and Technology in the year 2001. Rijndael is a family of block ciphers with different block sizes as well as different key length.

This paper at first briefly describes history of AES and the research works that have been done in the past years in the field of satellite data security using different proposed algorithms including AES. This leads to the proposed work in Sect. 2 where each step of our proposed cryptosystem is described. Section 3 discusses about the need of AES-256 algorithm for the security of remote sensing data. And finally, Sect. 5 concludes the paper.

1.1 Advanced Encryption Standard (AES)

During the selection process, The National Security Agency (NSA) reviewed all the AES finalists including Rijndael and said they were secure enough to implement for the encryption of the unclassified documents. However after rigorous testing in May 2002, the Rijndael algorithm was selected as the most suitable of all and hence became effective as Federal Government standard. AES is also listed in ISO/IEC 18033-3 standards and is first and only of its kind to be publicly available block ciphers for top-level security information approved by NSA. Rijndael was accepted as AES with three variants of 128-, 192-, 256-bit key size with block size of 128 bits. The design and strength of all keys of AES algorithm (i.e. 128, 192, 256) are sufficient to protect classified information up to SECRET level. However, 192- or 256-bit key should be used for top secret-level information [2]. AES uses 10, 12, 14 rounds for 128-, 192- and 256-bit keys for encryption, respectively.

1.2 Related Works

AES algorithm, being a higher efficient algorithm proposed in data encryption, has been widely acceptable in the works implemented in the field of satellite data security mainly the image data security. Boukhatem Mohammed Belkaid, Lahdir Mourad and Cherifi Mehdi proposed a system to intensify the security of transmission of Meteosat images which was based on AES and RSA (Rivest–Shamir–Adleman) algorithm and the system creates a new password in every session of encryption [3]. Lijie Yin et al. introduced an encryption scheme that merges EZW and chaos theory for the encryption of remote sensing images that avoids transmission of multi-key [4]. In 2010, Muhammad Usama et al. explained a system based on idea of chaotic cryptography using multiple chaotic maps and external secret key for encryption and decryption of satellite images [5]. Xiaoqiang Zhang et al. proposed an encryption algorithm in hybrid domain and experimented on remote sensing images using DWT and PWLCM system [6]. Faruk Ahmed and E. N. Ganesh implemented the processing of remote sensing images by using watermarking and encryption algorithm [7]. Naida H. Nazmudeen and Farsana F. J. proposed the idea of combining DWT-DCT watermarking algorithm and AES encryption algorithm for the improvement of satellite image security [8]. A secure image transformation algorithm was presented by Rafeeque K. M. and S. Shiva Shankar and the transformed image was encrypted using remote sensing algorithm [9]. P. Gunavathy and A. Vinoth Kannan proposed the concept of enhancement and segmentation of a satellite image and encrypting that segmented image using RC4 algorithm (Stream Cipher) [10]. Pokhali Sayeda Roohi Banu presented a model of AES which is fault-tolerant based on Hamming error correction code for avoiding the corruption of satellite onboard data mainly due to the SEUs (single event upsets) [11]. Recently in 2018, NovelSat Satellite Technologies have launched ProtCASTER, a satellite broadcast solution that is a circuit implementation of AES-256 algorithm [12].

The increasing public and private data communication has also given rise to further space assets dependencies. Once data breach has happened, it becomes really notorious job for the respective country to deal with. The attacker or the adversaries can be anywhere in the range of the satellite beam coverage which is miles. Moreover, the attacked country has to face double jeopardy as the attack in outer space cannot surely be pointed out to a specific country. As it will not only pose threat to international political relations of the country but also the strategic advances could diminish. Many powerful countries have observed state-sponsored cyber attacks and the lack of any international law restricting attacks in space makes the space cybersecurity further vulnerable [13, 14]. The space cyber attacks in the present days cannot be legally penalised, so this leaves us with only option to safeguard our satellites with the best possible security. The need for securing the remote sensing data hence increases further as they carry more sensitive information as compared to others. So it is wise to establish a secure communication traffic to nullify any such malicious attacks posing threat to the national security jeopardising its place at international level. This has given rise to various methods of cryptography and data hiding techniques. The most refined and trusted algorithm is AES (Advanced Encryption Standard) with the variation of 256-bit key which is considered ‘unbreakable’.

2 Proposed Work

In this work, a secure satellite communication system based on AES algorithm is proposed which involves a secure channel that uses a 256-bit key. The proposed system is designed to secure the entire data traffic for the transmission of remotely

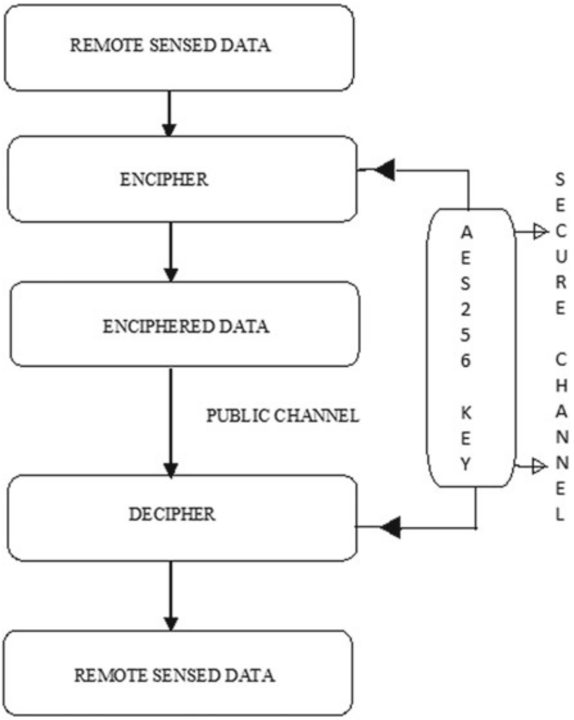


Fig. 1 Proposal framework

sensed data. The idea of implementing the scheme is laid out in the following flow chart (as shown in Fig. 1).

2.1 Remote Sensed Data

Remote sensing is the process of obtaining information about any object or surface phenomenon without establishing any physical contact with the object or its surface. The data acquisition for a particular object or phenomenon uses the principle of inverse problem. Sometimes, the parameters of the object or phenomenon in the particular area of interest cannot be measured directly. As a workaround to this, we acquire those parameters who have substantial relation with our area of interest, so that the required parameters can be estimated with maximum degree of certainty.

2.2 Encipher

During the data transmission to Earth stations, some losses are bound to happen due to channel noises and if the loss also incurs during the decryption, it would lead to an erroneous data keeping in mind the sensitivity of remote sensed data.

This would lead us to a trade-off between data security and data loss. Hence, the main idea is to use such algorithm that has the minimal chances of alterations being created in the image simultaneously ensuring that data security is also not jeopardised. This led us to AES-256 which successfully obliterates all the above concerns. In the proposed scheme, we intend to not only encrypt the message but instead the entire data traffic taking place between the satellite and the station.

The security of encryption can further be enhanced by adding several hashing methodology or coupling it with some competent encryption algorithm. However, this would depend on the design and demand of the remote sensing system as when and where it is implemented giving it a flexibility of adding or removing the security layers without much concern.

The encryption time for AES-256 is bit higher than its 128-bit counterpart due to more number of rounds involved in the encryption process. But it is still less than the other cryptographic modules. The security provided by AES-256 is much more higher than all of the existing modules and this has been justified in the later sections of the paper.

2.3 Decipher

This stage of the scheme will take place at the receiver end which can be earth station or any intermediate satellite. Decrypting follows the inverse algorithm of encryption (shown in Fig. 2). Since AES uses symmetric key, so we need to establish a secure channel to transfer the AES-256 key to the encipher stage of the scheme, making the keyless prone to attacks.

The transfer of key over a secured channel is to protect the key from any side-channel or known-key attacks. The key must be chosen wisely as side-channel or known-key attacks can some time bring down the brute-force attack time on any data communication channel. Let us assume if the attacker knows that the key bits are related to each other in some particular fashion then it becomes a relatively easy job as the brute force will have lesser domain of keys to search with. Therefore, if the keys are hashed and any related key is blocked by system in initial stage only, then it will almost completely nullify the chances of side-channel or known-key attacks. Moreover, the transfer of key over secured channel may be a subject to the data sensitivity of the information being transferred. The secured channel may or may not be a necessary subject for lesser sensitive or non-military grade data and may depend upon the demand and implementation of the project undertaken.

The following flow chart describes the AES-256 algorithm (shown in Fig. 2).

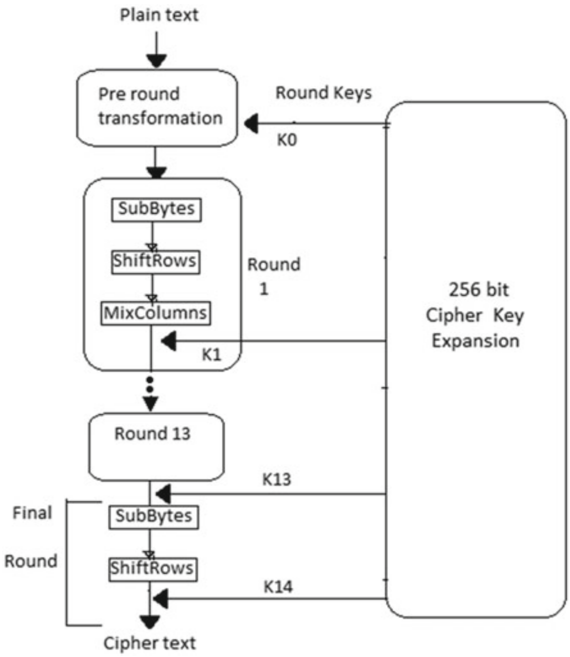


Fig. 2 Flow chart describing AES algorithm

3 Why AES-256 for Remote Sensing System

The proposed idea would affect the entire mechanism of remote sensing in a very significant way. As there are extra stages involved in the proposed mechanism, it is bound to create some overheads which may somewhat affect the efficiency of system, but addition of these extra security layers will weigh out the cons with it.

Many cryptographers and cryptanalysts term AES-256 bit as oversecure and rule out the possibility of 128-bit variant to be cracked and term it as safe for upcoming years. However, the term safe is relative and has no assurance of lifetime. Given the recent advancement if quantum computers come into existence, then it would not be an impossible task to carry out an attack on 128 bit but that would still take time even for 128-bit variant to be cracked. But this possibility is also ruled out because 256-bit variant will require more than twice the number of time taken to crack 128 bit. Remote sensing may have data security levels ranging from moderate to top secret-level. The proposed idea is robust enough to be implemented as a single module as well as holds the power to be coupled with other add-ons like hashing and hybrid cryptography to completely nullify the security vulnerabilities.

3.1 Implications on Remote Sensed Data

In the proposed work under the section of encipher, it is discussed that how the data sensitivity of remotely sensed data becomes inevitable when it comes to encryption and decryption and thus we chose AES to be best suited for the job. In comparison with AES-128, AES-256 stands out in terms of security but at the cost of speed and memory. Speed and memory overhead for AES-256 do not show a vast system requirement in terms of chip area and hardware installations. This trade-off between security and time and memory can easily be narrowed down with help of efficient designs and it is not of much concern given the recent technological advancements in chip fabrications. The implementation of design will take into account the demand of the remote sensing system in determining the security layers as mentioned in the proposed idea. For example, if the remotely sensed data has a higher military grade information, then it is wiser to add more security layers where security supersedes all the other factors, whereas this may not be the case for a topographic mapping satellite as it would require fewer layers of security.

3.2 Attacks and Vulnerability

AES has a comparatively simple algebraic framework. This property of AES was targeted in the XSL attack done by Nicolas Courtois and Josef Pieprzyk to expose the less complexity of the nonlinear components of the cipher [15]. However, the other follow-up papers have shown that the attack suggested by Courtois is impractical and hypothetical. The concern was raised by several other developers of the competing algorithm over the simplicity of nonlinear components of the Rijndael. The developer of competing algorithm Twofish, Bruce Schneier wrote that successful attacks on Rijndael would be developed someday but did not believe that anyone would ever discover the attack that could reveal the Rijndael traffic.

Some related-key attacks done by famous cryptographer Adi Shamir against AES-256 required 2^{39} time for key recovery in nine-round version, 2^{45} time for ten-round version [16] with a stronger related-key attack than the previous one. This becomes ineffective against AES-256 with 14 rounds and this can be completely nullified if full AES is implemented where the generation of the related key is constrained by proper software implementation. The key-recovery attacks and known-key distinguishing attacks on full AES have shown huge time and memory requirements to be utilised for the lower variants of the AES but that would still take billions of years to do brute-force attack and on the implementable hardware. These attacks are thus ruled out as these are impractical in nature and hence pose no threat to AES with 256-bit key [17].

Certain side-channel attacks have claimed to expose the AES-256 key but that requires the running of programme on the same node as the data. These attacks can also be nullified by having built-in hardware instructions for AES that will prohibit and safeguard against any timing-based side-channel attacks on AES.

4 Implementation Results

In the implementation of the project, we have coupled AES-256 with SHA 256 to perform hashing of the 256-bit key. Hashing improves the key strength and minimises any related-key attacks. The key entered by the user is padded to 256-bit key by using the hashing algorithm. We have coupled AES with (2, n) share cryptography. In this algorithm, we have divided the encrypted image into two shares (shown in Fig. 4). If either of the image share is lost, the remaining would be useless. The image shares would not reveal any data unless the other share is combined with it to produce the original encrypted image. This image sharing technique was suggested by Naor and Shamir [18]. The project was implemented to demonstrate the flexibility of the proposed algorithm as it can support hybrid cryptography and can be coupled with other algorithms also for better security layers in the communication channel.

The execution time for encryption using 256-bit key is more as compared to for the 128-bit variant due to more number of rounds involved in encryption of 256-bit variant. This leads to a trade-off between security and efficiency. However, the overheads involved in the process can be minimised by having upgraded hardware support which may incur some cost overheads leading to a triangular trade-off between cost, speed and security.

The proposed idea was implemented using python and python packages coupled with hashing (SHA 256) and visual cryptography by image sharing. The programme was implemented on Intel i3-380M CPU with 3M cache and clock rate of 2.53 GHz aided by 6 GB RAM. Figures 3, 4 and 5 are the results of our implementation of the proposed system. Figure 3 represents the input image which is encrypted using 256-bit key and image sharing technique represented as in Figs. 4 and 5 shows the decrypted image.

5 Conclusion

In this paper, we have tried to layout and implement a model for a secure data transmission in remote sensing by using Advanced Encryption Standard with 256-bit key size. We have tried to show why AES-256 is still now one of the safest cryptographic algorithms for the use of encryption and decryption. This moreover justifies the implementation of AES-256 in our proposed scheme to not only make the data encrypted, but we try to bring the entire data traffic happening between the various layers and nodes of remote sensing under the umbrella of AES-256 keeping in mind the data sensitivity and efficiency of the communication in accordance with the proposed idea for remote sensing.

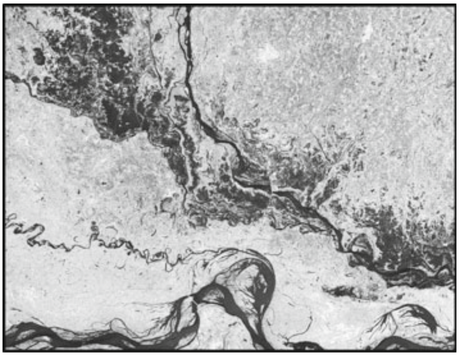
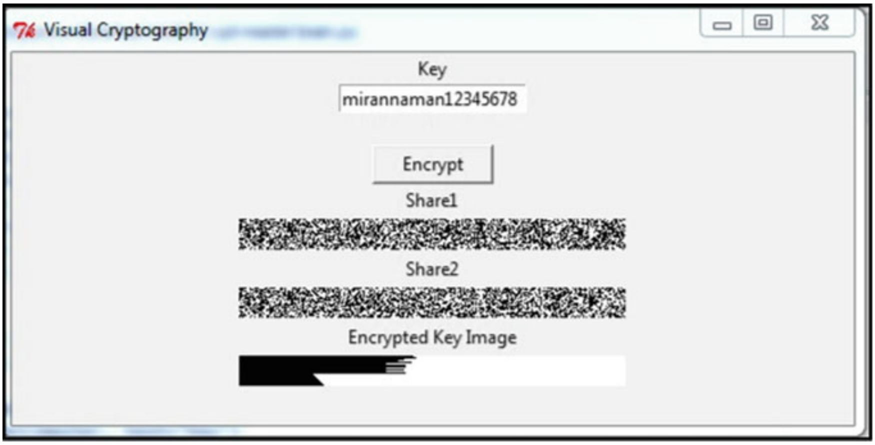


Fig. 3 Input image



Key

mirannaman12345678

Fig. 4 Encryption procedure with image sharing

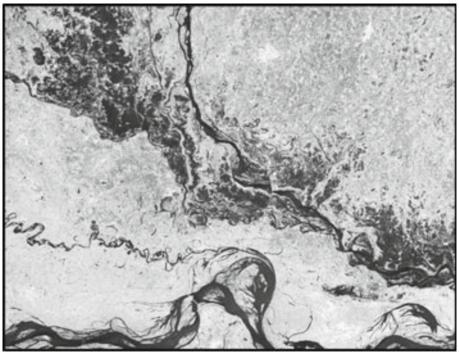


Fig. 5 Decrypted image

References

1. Tea Area Development and Management using RS and GIS | National Remote Sensing Centre, https://nrsc.gov.in/Tea_area
2. L. Hathway, *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information* (2003)
3. B. Mohammed, L. Mourad, C. Mehdi, Meteosat images encryption based on AES and RSA algorithms. Int. J. Adv. Comput. Sci. Appl. **6** (2015)
4. L. Yin, J. Zhao, Y. Duan, Encryption scheme for remote sensing images based on EZW and Chaos, in *2008 The 9th International Conference for Young Computer Scientists* (2008)
5. M. Usama, M. Khan, K. Alghathbar, C. Lee, Chaos-based secure satellite imagery cryptosystem. Comput. Math Appl. **60**, 326–337 (2010)
6. X. Zhang, G. Zhu, S. Ma, Remote-sensing image encryption in hybrid domains. Opt. Commun. **285**, 1736–1743 (2012)
7. F. Ahmed, D. Ganesh, Implementation of encryption and watermarking algorithm for remote sensing image. Int. J. Eng. Comput. Sci. (2016)
8. N. Nazmudeen, F.J. Farsana, Satellite image security improvement by combining DWT - DCT watermarking and AES encryption. Int. J. Adv. Comput. Res. **4** (2014)
9. R. Km, S. Shankar, Secure image transformation using remote sensing encryption algorithm. Int. J. Sci. Eng. Res. **5** (2014)
10. P. Gunavathy, A. Kannan, Segmentation and encryption of satellite images using stream cipher algorithm. Int. J. Comput. Sci. Mob. Comput. **5**, 743–750 (2016)
11. P.R. Banu, Satellite On-Board Encryption (2007)
12. NovelSat | NovelSat ProtCASTER, http://novelsat.com/novelsat-protcaster/
13. China-based hacking campaign is said to have breached satellite, defense companies, https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html
14. E. Rosenfeld, US weather systems hacked by Chinese: Report, https://www.cnbc.com/2014/11/12/chinese-hack-us-weather-systems-satellite-network-washington-post.html
15. B. Schneier, Crypto-Gram. 15 Sept 2002 - Schneier on Security, https://www.schneier.com/crypto-gram/archives/2002/0915.html
16. A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, Key Recovery Attacks of Practical Complexity on AES Variants With up to 10 Rounds (2010)
17. J. Goldberg, AES Encryption isn't cracked, https://blog.agilebits.com/2011/08/18/aes-encryption-isnt-cracked/ (2011)
18. M. Naor, A. Shamir, Visual cryptography, advances in cryptology, in *Eurocrypt'94 Proceeding LNCS*, 950. 1–12 (1995)