Satellite Imagery Security Application (SISA)

Mohammed Khan

Abstract— With the large-scale research and development in space sciences, space technologies, and network communication technologies, there is a great demand of satellite imagery security system for providing secure storage and transmission of satellite imagery over internet and/or shared network environment. This brings new challenges to protect sensitive and critical satellite imagery from unauthorized access and illegal use in order to keep the storage and transmission process secure and reliable. Therefore, there is strong need of satellite imagery encryption and decryption application for security. Satellite Imagery Security Application (SISA) is an information security application developed for satellite imagery. The application supports new and modified version two most popular data encryption standards named as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). This paper investigates the security and performance level of the new modified version DES and AES for satellite imagery. The method of application of DES and AES on the satellite imagery in each case is explained. The application provides conventional tools of measurement and analysis such as key sensitivity, statistical and performance analysis to determine the level of security, reliability and performance.

I. INTRODUCTION

Space sciences and technologies have recently attracted interest from researchers and industrial communities, mainly because of large number of possible applications capable to exploit remotely sensed data and images [1]. Emerging of these technologies present new opportunities for users to increase productivity, reduce costs, facilitate innovation and create virtual collaborative environments for addressing the new challenges. Remote sensing technologies, along with related geospatial technologies, contribute powerful tools for preserving and protecting the nation's critical infrastructure [2]. In these systems, the data storage and transmission process, mainly based on CD/DVD-ROM hardcopy and/or shared network environment, provides the user with a digital version of the satellite imagery. Therefore, there is an inherent risk of unauthorized access or illegal use of the images. In addition, there is a dire need of security and privacy for all information systems in the digital world [12]-[25].

Recently many text data and multimedia image encryption schemes have been proposed using DES and AES algorithms, and some of them have been extended from text data to multimedia image encryption. A direct extension of the text data and multimedia image encryption scheme works also for satellite images, but this simple modification may not provide

an efficient solution to the concerned satellite image encryption problems because satellite imagery has its own specifications for encryption such as speed, compatibility to image format and compression standards, and real-time implementation etc., therefore requires a special design of the encryption algorithm while dealing with high resolution and multi-spectral satellite imagery.

In this paper, we address aforementioned issues and develop the satellite imagery security application to eliminate associated problems for satellite imagery. To achieve this, we investigate the simulation results of SISA encryption application to measure the security and performance level of the DES and AES encryption techniques for satellite imagery. The SISA is a powerful satellite imagery protection application, yet simple to deploy and use, extensible SISA solutions meet a variety of needs.

II. OVERVIEW ON THE ENCRYPTION ALGORITHMS

This section will provide a brief overview on the implementation and construction method of DES and AES encryption algorithms for satellite imagery.

A. DES Satellite Image Encryption

The most widely used symmetric block cipher is based on the DES which consists of SimpleDES and TripleDES algorithms. As with any symmetric encryption technique, in DES two inputs are the subjected for encryption and decryption process. The first is plaintext/image to be encrypted and the second is secret key. In this case, the original plaintext/image data is divided into equal length 64-bit blocks then the 64 bits block passes through DES encryption/ decryption function. The encryption/decryption process is based on 64 bits complex key-dependent computation operation. The encryption/decryption operation continues until all the input blocks of the plaintext/image passes through encryption/decryption function using same input secret key.

B. TripleDES Satellite Image Encryption

SimpleDES uses 56 bits key for encryption which is not suitable against attacks like brute force. TripleDES resolves this key space issue by increasing the key space without switching to another algorithm. TripleDES is more intensive and stronger than SimpleDES. The single encryption/decryption operation of TripleDES is a combination of three SimpleDES operations. Let assume that SimpleDES encryption

Figure 1. SISA properties dialog for performing encryption operation

and decryption operations are define as $EK(I)$ and $DK(I)$ respectively using I as input block and K as secret key.

The TripleDES encryption of a 64-bit block I into a 64-bit block O is defined as [3].

$$O = E_{K3}(D_{K2}(E_{K1}(I))) \quad (1)$$

$$I \rightarrow \text{DES } E_{K1} \rightarrow \text{DES } D_{K2} \rightarrow \text{DES } E_{K3} \rightarrow O$$

The TripleDES decryption of a 64-bit block I into a 64-bit block O is defined as [4]

$$O = D_{K1}(E_{K2}(D_{K3}(I))) \quad (2)$$

$$I \rightarrow \text{DES } D_{K3} \rightarrow \text{DES } E_{K2} \rightarrow \text{DES } D_{K1} \rightarrow O$$

Where $K1, K2$ and $K3$ are the input keys for TripleDES encryption and decryption operation and can be used with different options e.g. $K1, K2$ and $K3$ are independent keys; $K1$ and $K2$ are independent keys and $K3 = K1$; and $K1 = K2 = K3$.

C. AES Satellite Image Encryption

The AES is an iterative symmetric block cipher for data encryption developed by Joan Daemen and Vincent Rijmen. The AES algorithm is flexible to support variable block and key length. AES algorithm supports 128, 192 or 256 bits input block, output block and State. The State is divided into four operational blocks and organized in 4×4 bytes of array where number of columns in state matrix is $NC = 4$ and with key size K of length $NK = 4, 6$ or 8 respectively, which reflects the number of 32-bits or number of columns in the Key.

Figure 2. Structure of AES Encryption algorithm for Satellite Imagery

The key length suggests number of rounds NR required by algorithm to perform encryption/decryption operation. If $NR=10$ then $NK = 4$, if $NR=12$ then $NK = 6$ and if $NR=14$ then $NK = 8$. The supported key length, block size and number of rounds combinations are given in Table 1. The AES key size is long enough to resist against attacks like brute force. AES algorithm is flexible, reliable and gives good performance for its hardware implementation [5]–[8]. Today, AES algorithm performs well for applications that need fast computation and processing e.g. smart cards, cellular phones, image-video encryption etc. [9]

The AES algorithm uses round function for encryption/decryption. The round function put together four

Figure 3. Encrypted Satellite Image.

transformation operations Byte substitution transformation, Shifting rows transformation, MixColumns transformation and AddRoundKey transformation. The decryption structure has exactly the same sequence with inverse transformation as the one in the encryption structure. The encryption procedure consists of several steps as shown by Figure. 2.

	Key Length (<i>NK</i> words)	Block Size (<i>NC</i> words)	No. of Rounds (<i>NR</i>)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

III. SECURITY ANALYSIS

A good encryption algorithm or technique should resist all kinds of known attacks, such as known-plain-text, cipher-text, statistical analysis and brute-force attacks. Therefore quantitative measuring techniques are needed to be considered for evaluation of satellite imagery encryption quality. Some of the statistical analysis techniques described in this paper are most well-suited for security and performance level of satellite imagery. The methods described here are found in SISA application for measuring security and performance level of the SimpleDES, TripleDES and AES. In this paper, we use the gray-scale Boston image of size 1000 x 1000, gray-scale as the original image depicted in Figure 7(a). The encrypted and decrypted images are depicted in Figures 4, 5 and 6. As shown, the encrypted images are totally scrambled and invisible. The decryption process takes encrypted image as input, together with the same sized (which is 256 bits) secret key the output decrypted images are shown in Figures 4(b), 5(b) and 6(b).

A. Histograms Analysis

The histogram of a Boston image (shown in Figure 7(b)) contains very high heels of spikes. The encrypted images and the corresponding histogram images using these algorithms under CBC mode are shown in Figure 8. These histograms are more uniform, significantly different from that of the original Boston image, and have no similarity with the original Boston image. Hence does not have any clue for statistical attack.

B. Keyspace Analysis

A good encryption algorithm should be sensitive to the secret key, and the keyspace should be large enough to make brute-force attack infeasible and impracticable. For the SimpleDES, TripleDES and AES satellite image encryption algorithm, some basic analysis and test results are summarized as follows:

1) Number of Control Parameters

The SimpleDES is designed to encrypt/decrypt blocks of input data of 64-bits using 56-bits key. The small 56-bits key of DES can be broken by brute force in a relatively short time. TripleDES resolves key space issue of the Simple-DES by increasing the key space without switching to another algorithm and it operates with 64, 128 and 192 bits key whose key space size is 2^{56} , 2^{128} and 2^{192} . As compare to these two algorithms, AES have long enough key space to resists against brute force which is 2^{128} , 2^{192} and 2^{256} .

(a) Encrypted Image (b) Decrypted Image

Figure 4. Encrypted and Decrypted image of SimpleDES under CBC Mode with 64-bits Key and Block size.

(a) Encrypted Image (b) Decrypted Image

Figure 5. Encrypted and Decrypted images of TripleDES under CBC Mode with 128-bits Key and 64-bits Block size.

(a) Encrypted Image (b) Decrypted Image

Figure 6. Encrypted and Decrypted images of TripleDES under CBC Mode with 128-bits Key and 64-bits Block size.

2) Key Sensitivity Test

An ideal image encryption algorithm procedure should be sensitive to the secret key. The change of a single bit in the secret key should produce a completely different output results. To prove the robustness of the AES algorithm, the key sensitivity analysis has been performed. Assume that a 32-character secret key is used. This means that the key consists of 256-bits. A typical key sensitivity test is performed according to the following steps:

First, a 512 x 512 image in Figure 9(a) is encrypted by using the test key “12345678901234567890123456789012” in ASCII. The output encrypted image is shown in Figure 9(b) referred as Image A. Then, the least significant bit of the key is changed, so that the original key becomes “22345678901234567890123456789 012” in this example,

which is used to encrypt the same image. The output encrypted image is shown in Figure 9(c) and referred as image B.

(a) Original Image

(b) Histogram of original Image

Figure 7. Boston satellite image and its corresponding histogram

(a) Encrypted and Histogram Images of SimpleDES with 64 bits Key

(b) Encrypted and Histogram Image of TripleDES with 128 bits Key

(c) Encrypted and Histogram Image of AES with 256 bits Key

Figure 8. Histograms and Encrypted images of SimpleDES, TripleDES and AES under CBC Mode

Again, the same original image is encrypted by making the slight modification in the secret key i.e. secret key “12345678901234567890123456789033” in ASCII (the least significant bit is changed in the secret key) and the output encrypted image is referred as encrypted image C as shown in Figure 9(d).

Finally, the above three encrypted images A, B and C, encrypted by the three slightly different secret keys, are compared for analysis with original image. It is not easy to compare these images visually. So for comparison, we have

calculated the correlation coefficient and maximum deviation between the pixel values of the three encrypted images (is given in Table 2).

Figure 9. Key sensitive test of AES algorithm

C. Correlation of Pixels Between Original & Encrypted or Decrypted Images

Correlation is a measure of the relationship between two variables. The correlation coefficient is measured using equation (3) [11]. To test the correlation between pixel values of the encrypted and original images, the procedure is as follows:

$$\text{Correlation Coefficient} = \frac{\text{cov}(x, y)}{\sigma_x \sigma_y}$$

$$= \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N (x_i - E(x))^2} \sqrt{\sum_{i=1}^N (y_i - E(y))^2}} \quad (\square 3)$$

The computed correlation coefficient values of the adjacent pixels of experimental images using SimpleDES, TripleDES and AES under CBC mode of operation are given in Tables 3, 4, 5, 6 and 7. All the experiment results of encryption process have less or greater values from zero and no one have 1 or -1 values its means these encryption algorithms are secure from statistical attacks. The computed correlation coefficient values of decryption process are approximately near to 1 (little change is computed values is negligible) which mean that decryption

process executed successfully. The original image and decrypted images are identical to each other.

TABLE 2. MAXIMUM DEVIATION AND CORRELATION COEFFICIENTS CALCULATION OF THE THREE ENCRYPTED IMAGES USING AES ALGORITHM SHOWN IN FIGURE 9.			
Image 1	Image 2	Correlation Coefficient	Maximum Deviation
Encrypted image A Figure 9(b)	Encrypted image B Figure 9(c)	-0.000408	11196331
Encrypted image B Figure 9(c)	Encrypted image C Figure 9(d)	0.000310	11176711
Encrypted image C Figure 9(d)	Encrypted image A Figure 9(b)	0.0015	11185447

D. Information Entropy Analysis

The information entropy $H(m)$ of the image m can be calculated as: [12]

$$H(m) = \sum_{i=0}^{2N-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (4)$$

Where $P(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e. $m = \{m_1, m_2, \dots, m_{2^8}\}$. After evaluating above equation, we obtain its entropy $H(m) = 8$, corresponding to a truly random source. However, when the images are encrypted, their entropy should ideally be 8. If the output of such encryption emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Let us consider the encrypted images of SimpleDES, TripleDES and AES algorithms under CBC mode of operation, the number of occurrence of each encrypted image is recorded and the probability of occurrence is computed. The computed entropies of encryption and decryption processes are listed in Tables 3, 4, 5, 6 and 7. The values obtained of encryption process are very close to the theoretical value 8. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack.

TABLE 3: QUALITY MEASURES FOR SIMPLEDES UNDER CBC OPERATIONAL MODE.			
Operation	Seconds	Entropy	Correlation
Encryption	5.31	7.9998	-0.0005
Decryption	5.42	7.5583	1

TABLE 4: QUALITY MEASURES FOR TRIPLEDES ENCRYPTION PROCESS UNDER CBC OPERATIONAL MODE.				
Block Size	Key Size	Seconds	Entropy	Correlation
64	128	5.52	7.9998	0.0006
64	192	5.53	7.9998	0.0005

TABLE 5: QUALITY MEASURES FOR TRIPLEDES DECRYPTION PROCESS UNDER CBC OPERATIONAL MODE.				
Block Size	Key Size	Seconds	Entropy	Correlation
64	128	5.53	7.5583	1
64	192	5.5	7.5583	1

TABLE 6: QUALITY MEASURES OF AES ENCRYPTION OPERATION UNDER CBC MODE WITH DIFFERENT BLOCK AND KEY SIZES.				
Block Size	Key Sizes	Seconds	Entropy	Correlation
128	256	0.47	7.9998	-0.0008
192	256	0.47	7.9998	-0.0009
256	256	0.45	7.9998	-0.0009

TABLE 7: QUALITY MEASURES OF AES DECRYPTION OPERATION UNDER CBC MODE WITH DIFFERENT BLOCK AND KEY SIZES.				
Block Size	Key Sizes	Seconds	Entropy	Correlation
128	256	0.33	7.5588	0.9998
192	256	0.3	7.5588	0.9998
256	256	0.3	7.5588	0.9998

E. Performance Evaluation

Apart from the security analysis by evaluating statistical analysis and measurements, some other very important issues on satellite image encryption/decryption are needed to be considered. These issues include the performance and efficiency for real-time application while doing satellite image encryption/decryption. The application of proposed algorithm is implemented using the Matlab, Microsoft C# .Net programming language and performance of algorithm is observed on a Pentium-IV 1.8 MHz PC with 1.46 GB RAM running Microsoft Windows 2003 server Enterprise Edition. Results of some experiments are given to prove the good performance, efficiency and security of AES algorithm for satellite images. The modified AES satellite image algorithm is very fast as compare to other traditional satellite image encryption algorithms like SimpleDES and TripleDES algorithms. In addition, to improve the accuracy of our timing measurements of proposed algorithm, each set of the timing tests shown in Table 8, was executed 5 times, and we report the average of the times thereby obtained.

TABLE 8: COMPARATIVE SPEED TEST OF EXPERIMENT RESULTS ON BOSTON SATELLITE IMAGE. (TIME IN SECONDS)			
	SimpleDES	TripleDES	AES
Avg. time taken for Encryption	5.42	5.76	0.44
Avg. time taken for Decryption	5.47	5.73	0.46
Max. time taken for Encryption	5.53	6.14	0.56
Max. time taken for Decryption	5.61	6.10	0.56
Min. time taken for Encryption	5.31	5.52	0.38
Min.time taken for Decryption	5.39	5.50	0.41

IV. CONCLUSION

Due to the increasing use of satellite imagery in research, academics, industries etc, we need an application which can

protect sensitive, critical and secret data from the unauthorized access and illegal use, in order to keep the data storage and transmission process secure and reliable over shared network environment or Internet. The security of high resolution and multi-spectral satellite imagery is very difficult from text and images because of its intrinsic characteristics, features and formats. In such case the encryption/decryption speed and algorithm simplicity are usually considered more important for any security application. In this paper, comprehensive theoretical and experimental analysis of modified SimpleDES, TripleDES and AES encryption techniques for satellite imagery using SISA application have been described in brief. The analysis tools of the SISA application such as key space, key sensitivity, correlation coefficient, information entropy and performance evolution analysis have been performed to measure the security and performance level of these algorithms for satellite imagery. The experimental results demonstrate that AES is very fast symmetric block cipher and operates with 128, 192 or 256 bits keys. Therefore, we can conclude that SISA application has provided a low-maintenance way to safeguard sensitive satellite imagery while proactively laying the foundation for future security needs. Detail analysis and experiment results prove that application provides strong and long-term data security solution for satellite imagery.

REFERENCES

- [1] Mauro Barni, Franco Bartolini, Enrico Magli and Gabriella Olmo, "Watermarking techniques for electronic delivery of remote sensing images", Optical Engineering, vol. 41, no. 9, pp. 2111-2119, September 2002.
- [2] Ray A. Williamson, "Remote Sensing and Transportation Security", Pecora 15/Land Satellite Information IV/ISPRS Commission I/FIEOS Conference Proceedings, 2002.
- [3] Federal Information Processing Standards Publication, FIPS PUB 46-3, "Data Encryption Standard (DES)", January 1977, Reaffirmed: October 1999.
- [4] Federal Information Processing Standards Publication, FIPS PUB 197, "Advanced Encryption Standard (AES)", November 2001.
- [5] K. Gaj, P.Chodowiec, "Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays" in: CT-RSA, pp.84-99, 2001.
- [6] Hodjat, I. Verbauwhede, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA", Proceedings of the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM), pp. 308-309, April 2004.
- [7] K. Janvinen, M. Tominisko, J. Skytta, "A fully pipelined memorlyess 17, 8 Gpbs AES-128 cryptor", International symposium of Field programmable Gate arrays, pp.207-215, 2003.
- [8] M. McLone, J.V. McCanny, "Rijndael FPGA implementations utilizing look-up tables", J.VLSI signal process, system, vol. 34, no. 3, pp. 261-275, 2003.
- [9] Federal Information Processing Standards Publication, FIPS PUB 197, "Advanced Encryption Standard (AES)", November 2001.
- [10] Nawal El-Fishawy and Osama M. Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, vol. 5, no. 3, pp. 241-251, November 2007.
- [11] Tao Xiang, Xiaofeng Liao, Guoping Tang, Yong Chen, Kwok-wo Wong, "A novel block cryptosystem based on iterating a chaotic map", Elsevier B.V., Physics Letters A, vol. 349, pp. 109-115, 2006.
- [12] Horng, S.J. Tzeng, S.F. Pan, Y. Fan, P. Wang, X. Li, T. Khan, M.K, "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET", IEEE Transactions on Information Forensics Security, 2013, 8, 1860-1875.

- [13] Z. Liu, X. Huang, Z. Hu, M.K. Khan, H. Seo, L. Zhou, "On emerging family of elliptic curves to secure internet of things: ECC comes of age", *IEEE Transactions on Dependable and Secure Computing*, pp. 99, 2017, pp. 237-248
- [14] S.F Tzeng, S.J Horng, T. Li, X. Wang, P.H. Huang, M.K Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET", *IEEE Transactions on Vehicular Technology*, vol 66, no. 4, pp. 3235-3248, 2017
- [15] A.K Das, M. Wazid, N. Kumar, M.K Khan, K.W.R Choo, Y.H Park, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment", *IEEE Journal of Biomedical and Health Informatics*, vol. 22, issue 4, pp. 1310-1322, 2017
- [16] P.W Tsai, M.K Khan, J.S Pan, B.Y Liao, "Interactive Artificial Bee Colony Supported Passive Continuous Authentication System", *IEEE Systems*, Vol. 8, Issue, 2, 2014
- [17] F. Wu, L. Xu, S. Kumari, X. Li, A.K. Das, M.K Khan, M. Karuppiah, R. Baliyani, "A Novel and Provable Authentication and Key Agreement Scheme with User Anonymity for Global Mobility Networks", *Security and Communication Networks*, 2016
- [18] I. Uddin, M. Guizani, B.S Kim, S. Hassan, M.K Khan, "Trust Management Techniques for the Internet of Things: A Survey", vol. 7, pp. 29763-29787, *IEEE Access*, 2018
- [19] A.S Tolba, M.K Khan, Khaled A, "Systems and Methods for Three-Factor Authentication", US Patent No. 8862888, 2014
- [20] M.K Khan, "Fingerprint Biometric-based Self and Deniable Authentication Schemes for the Electronic World", *IETE Technical Review*, vol. 26, issue 3, pp. 191-195, May-June, 2009
- [21] A. Waqar, A. Raza, H. Abbas, M.K Khan, "A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata", vol. 36, issue 1, pp. 235-248, *Journal of Network and Computer Applications*, 2013
- [22] M.K Khan, K. Alghathbar, "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'", *Sensors*, vol. 10, Issue 3, pp. 2450-2459, 2010.
- [23] S. Kumari, M.K Khan, R. Kumar, "Cryptanalysis and improvement of 'a privacy enhanced scheme for telecare medical information systems'", *Journal of medical systems*, vol. 37, issue 4, 2013
- [24] V. Odelu, A.K Das, M.K Khan, KKR Choo, M. Jo, "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts", vol 5, pp. 3273-3283, *IEEE Access*, 2017
- [25] D. He, H. Wang, MK Khan, L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography", vol. 10, issue 14, *IET Communications*, 2016