International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 8059-8072

http://www.ripublication.com

Multi-Level Chaos Based Encryption Mechanism to Enhance Security of High Security Zone Areas on Google Map Satellite Images of India

Rajesh Duvvuru[1], P. Jagadeeswara Rao[2], Gudikandhula Narasimha Rao[3], Lasya Venigella [4] and YLN Swami P[5]

[1,2,3,4]Department of Geo-Engineering,
College of Engineering, Andhra University
Visakhapatnam, Andhra Pradesh, India
Email: {rajesh.duvvuru[1], lasyapadmaja@gmail.co[4]}@gmail.com
pjr_geoin@rediffmail.com[2], narasimha.geo@cea.auvsp.edu.in[3]
[5]Department of Spatial Information Technology,
University College of Engineering, JNTU Kakinada,
Kakinada, Andhra Pradesh, India
Email: yogananda.india@gmail.com[5]

Abstract

Confidentiality and reliability are two vital parameters for the Remote sensing data. Due to the wide range of applications of Remote Sensing and Geographical Information Systems (RS &GIS) in space sciences, it got more popularity in the recent times. Principally Remote Sensing has enabled mapping, studying, monitoring and management of various resources like agriculture, forestry, geology, water, ocean etc. Especially secure Remote sensing images transmission over network is still a major challenge for the researchers and practitioner. This work introduces a novel Chaotic Multi-level Remote Sensing Data encryption (CMRSDE) algorithm for the more security of Remote sensing images. CMRSDE algorithms comprises of Chaos based crypto system in Digital Signal Processing (CDSP) and Selective Encryption (SE) algorithm. SE algorithm, Cubic map and Logistic map are applied on Remote Sensing images and resultant image is subjected for the CDSP process. The simulations were conducted with the help of Matlab. The implementation was developed individually, later we merged the performance. Data rate, Total Encryption time and size of the image are three major parameters that are taken into consideration for the performance evaluation of the CMRSDE mechanism. Experimented results were compared with the non-chaos based technique like RSA algorithm and Selective Chaos and Non-

Selective Chaotic based algorithms. The experiment results proved that proposed CMRSDE algorithm performs better than existing non-chaos based techniques.

Introduction

Terror attacks, Naxal attacks are serious problem, which are to be considered. Globally, none of the country is exempted from this grave issue especially in India. This results a great loss of innocent mankind on this Earth. For instance, in 26/11 Mumbai attacks, terrorist used Google Earth satellite images and executed terror attacks, this results death of approximately 164 valuable human lives [1]. According to the Indian security intelligence agencies popularly known as Research analysis and Wing, it states that more attack is planned in near future by different terror attacks in high secured zones in India. Latest Banglore serial blast on 28/12/2014 is one among them. Satellite images of Earth data are playing a key information source for the extremist's. In general, Satellite images also called as Remote Sensing Images (RSI). Due to the extensive usage of RSI data, it has many applications like aerial early warning, traffic control, certain large scale meteorological data, Also in ocean waves metrics resembling altimeters measure, wind speeds direction, surface ocean currents and its directions and many more [2]. According to Campbell, basically Satellite image date were classified into five different types, they are temporal, spectral, radiometric, Geometric and spatial [3]. These images are used according to their need. In general remote sensing images are stored in database or data warehouse and certain clustering and classification techniques are applied on RS data for the image analysis [28][29][30]. For instance spatial resolutions are used for representation of surface area. Then, spectral resolution is defined by the wavelength interval size and number of intervals. Whereas, temporal RSI data is refers by amount of time (eg. Days). Then, Radiometric resolution defines as effective bit-depth of the sensor (No. of grayscale levels) and is usually expressed as 8-bit (0-255), 11-bit (0-2047), 12-bit (0-4095) or 16-bit (0-65,535).

Lastly, Geometric resolutions described as the satellite sensor's ability to effectively image a portion of the Earth's surface in a single pixel and are typically shown in terms of Ground Sample Distance (GSD)[4][5][6]. Many researchers and practitioner were discussed the importance of secure RSI and its applications using Chaos based approaches [7][8][9]. But the computation is high for those algorithms. Security need to be provided to RSI data, wherever the situation demands. But the existing algorithms secure unwanted data also, which intern increased the computation speed. If computation increases, it will reflect in wastage of all other parameters pertaining to computation like time, energy, large of volume of data, processing speed and other computational resources. To overcome the reliability, security and privacy issues of satellite imagery. This paper introduces novel Chaotic Multi-level Remote Sensing Data encryption (CMRSDE) algorithm. The proposed system is designed for improving the specific parameters like time and data size beside assuring security to RSI.

This work consists of: (1) a analysis and requirements of security for remote sensing data; (2) Chaotic Multi-level Remote Sensing Data encryption; and (3) a new measurements by integrating both security and performance; (4) a simulator where the CMRSDE algorithm were implemented and tested. The rest of this paper is structured as follows. Section 2 discusses previous works in the area of remote sensing, and Chaos based algorithms. Section 3 describe the architecture of proposed system. In section 4, it is simulation works were executed and performance evaluation of proposed algorithm is discussed. Finally, the paper is concluded with future scope discussed in Section 5.

Related Works

This chapter discusses the background works that pertaining to Remote sensing images, Google maps, Chaos theory, and high security zones in Andhra Pradesh. This work considered the two level selective chaos encryption algorithms.

Recently Geoff Groom et al. discussed the importance of remote sensing data, through object-based image analysis model on marine bird distributions and analysis [10]. Google maps and Google Earth are two rich information sources for collecting the satellite image data of specific area on this earth. The Google maps data were incorporated using NASA's Landsat satellite series, Oceansat series and DigitalGlobe's QuickBird satellite, MODIS and many other [11]. Currently the remote sensing data is sued for the simulation using Google's Earth using Image Landsat satellite. Landsat 8 Operational Land Imager (OLI) and Thermal Infrared Sensor (TIRS) images consist of nine spectral bands with a spatial resolution of 30 meters for Bands 1 to 7 and 9. New band 1 (ultra-blue) is useful for coastal and aerosol studies. New band 9 is useful for cirrus cloud detection. The resolution for Band 8 (panchromatic) is 15 meters. Thermal bands 10 and 11 are useful in providing more accurate surface temperatures and are collected at 100 meters. Approximate scene size is 170 km north-south by 183 km east-west (106 mi by 114 mi) [12]. LRA Narayan explain in detailed of about remote sensing data and its applications like forestry, agriculture, water, geology, ocean and more [13]. Muhammad Usama et al discussed the vital role of security to the remote sensing images and made an enormous study on chaos based RSI algorithms. The work describes different combination of chaos based algorithms like Cubic, Henon, Logistic, SINE, Tent and Cheybyshav maps. In addition to that, the encryption was done using multilevel encryption [7] [14]. Whereas Panduranga H T and NaveenKumar S K explained the importance of the selective encryption through chaos based Cubic Map and reduced the computation time [15]. According to the recent research reports and our investigations regarding bombast and terror attacks in India clearly shows the impact of terrorism in India [16]. In the literature of the security especially Wireless networks are more prone to the security. Our previous works describes certain solutions regarding security attacks, which refered for stregenthening the image security [24][25][26][27]. Majorly the proposed approaches discuses on two chaotic maps namely selective logistic and selective cubic maps. Logistic map technique is good one for preserving the image information through a chaotic behavior. N K Pareek et al discussed the encryption of chaotic based images using logistic map in detail [17]. Thomas D. Rogers describes the chaos Cubic mapping in the work, the even cubic mapping is older, but it is widely used [18]. The proposed technique is combines the features of Selective encryption, Logistic maps and Cubic map with respect to the multi level encryption on Satellite images. The rest of the algorithms were discussed in the section 3.

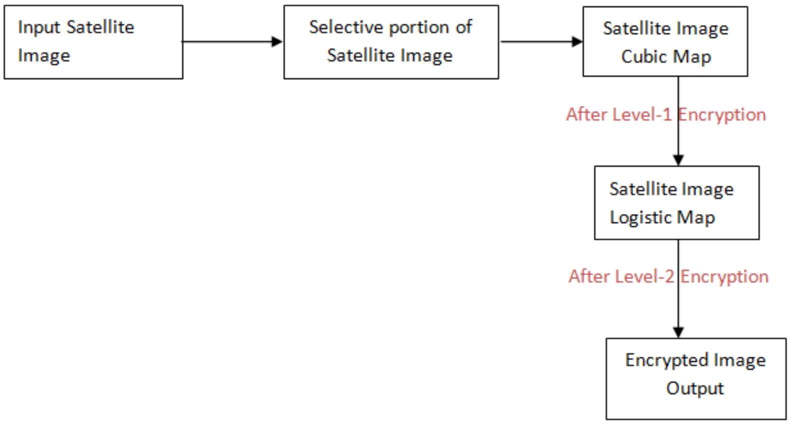


Figure 1: Block Diagram of Proposed System

The Multi-Level Remote Sensing Data Encryption (CMRSDE) Algorithm

Assumptions and Notations

The satellite maps of Andhra Pradesh were considered for the simulation. In that map, the some places were identified as High Security Zones (HSZ), like Naval Dock Yard, SHAR (ISRO), Tirumala region (Tirupati) etc. HSZ are bifurcated into Priority Privacy Zones (PPZ), where security needed. The blast places occurrence were assumed using Random Probability Distribution Function (RPDF). The keys K1 and K2 were selected Pseudo Random Number Generator (PRNG) [20]. State and Country information were collected and assumed as Raw Data (RD).

The computation time of the Region-of-interest (RT) [21] can be defined as

RT= ROI (x1,x2..xn) ---------- (1)

Where ROI is the function and x is the pixel position and values.

The computation time of the logistic map (LMT) can be articulated as

$$LMT = x_{n+1} = ax_n (1 - x_n) \text{ --------} \quad (2)$$

Where a is chaos behavioral variable and it value ranges from 3.5 to 4 and x = {1,2,3 ….n} is pixel coordinates, which will increase the population of the pixels.

The computation time of the cubic map (CMT) can be expressed as

$$CMT = x_{n+1} = ax_n (1 - x_n^2) \text{ ----------} \quad (3)$$

Where x = {1,2,3 ….n} is pixel coordinates which will increase the population of the pixels and a is chaos behavioral variable and it value is 2.59 .

The Total computation time of CMRSDE (CMRSDET) is uttered in equation 4.

$$CMRSDET = RT + LMT + CMT \text{ ---------} \quad (4)$$

Total computation Space (ST) occupied by the data by Selective Encryption (SE) and Non-Selective Encryption (NSE) can be defined as

$$ST = NSE - SE \quad \text{-------} \quad (5)$$

Finally CMRSDE Overall Performance (CMRSDEOP) can be referred as

$$CMRSDEOP = CMRSDET + ST \text{ ------} \quad (6)$$

The CMRSDE algorithm

This CMRSDE algorithm procedure is as follows:

Step1: Acquire the Input Image of HSZ region of RD from Google earth or Google map of LANDSAT satellites data.

Step2: Convert the HSZ Color Image jpg to HSZ Grey Scale Image.

Step3: Identify the PPZ area from HSZ map.

Step4: Select and Highlight the area of PPZ and save as image I1.

Step5: Apply the Cubic map bifurcation algorithm encryption on image I1 using PRNG key K1and save resultant image as I1

Step6: Apply the Logistic map encryption on image I1 using PRNG key K1and save resultant image I2, Where I2 is final encrypted HSZ image.

Step7: Exit and Stop procedure.

Simulation and Results

Data Acquisition

The simulated data is acquired from the Google maps [22], only a few places were selected as HSZ. The data were acquire with standard screen resolution of 1376 x 768 (HxV) pixels and For instant the Naval Dockyard, Visakhapatnam, Andhra Pradesh, Satellite image were selected and collected image. Where the spatial coordinates are 170 421 05.1511 N and 830 161 09.2011 E. And also elevation is 252 feet and image acquired from 15486 feet height. Table 1 specifies the data acquisition information, used for experimentation.

Table 1: Acquisition of HSZ Spatial Data

HSZ	Spatial Coordinates	Elevation (ft)	Eye alt (ft)
SHAR, Nellore	(13^0 42^1 54.44^{11} N, 80^0 13^1 58.94^{11} E)	23	8162
Naval Dockyard, Visakhapatnam	(17^0 42^1 5.15^{11} N, 83^0 16^1 09.20^{11} E)	252	15486
Tirumala Temple, Tirupati	(13^0 40^1 59.78^{11} N, 79^0 20^1 50.70^{11} E)	2835	6564

Simulation of CMRSDE using Matlab

Once the data acquired from the Google maps and it is stored in the PC. The PPZ portion is segmented using Region-of-Segmentation (ROI) algorithm from HSZ. Later Matlab simulation was performed on Logistic and Cubic maps. The computation time were calculated on the basic of the 4 GB RAM, Intel i3 processor and Matlab 7. The computation time depends on the processing speed.

Results and Discussion

Simulation Results of CMRSDE

The results that were performed on Matlab software were shown in the flowing tables 2 to 7. Table 2,4 and 6 shows the encryption of HZS data of SHAR, Tirumala and Naval Dockyard. Whereas Table 3,5 and 7 presents the data of PPS data of SHAR, Tirumala and Naval Dockyard.

Table 2: SHAR area of HSZ encryption with CMRSDE

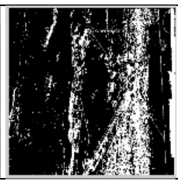
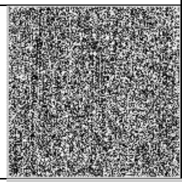
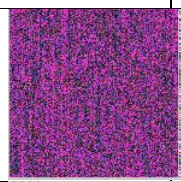
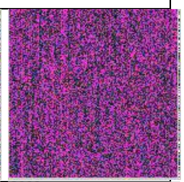
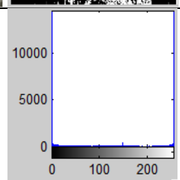
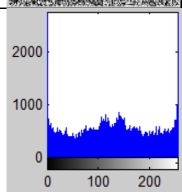
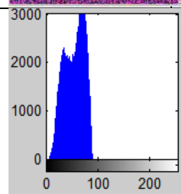
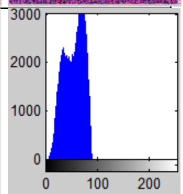
SHAR area HSZ Data Encryption	Input Satellite Image	Gray Scale Image	Cubic Map Encryption	Logistic Map Encryption	Final Output Image
Image					
Histogram Equalization	NIL				

Table 3: SHAR area of PPZ encryption with CMRSDE

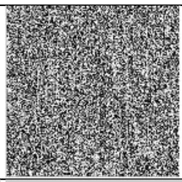
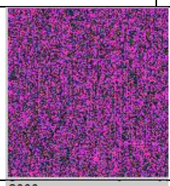
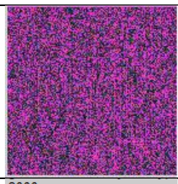
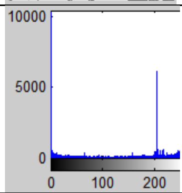
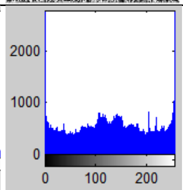
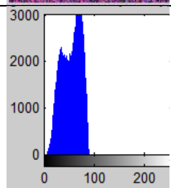
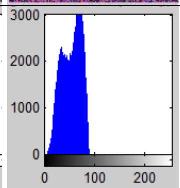
SHAR launch pad area PPZ Data Encryption	Input Satellite Image	Gray Scale Image	Cubic Map Encryption	Logistic Map Encryption	Final Output Image
Image					
Histogram Equalization	NIL				

Table 4: Tirumala area of HSZ encryption with CMRSDE

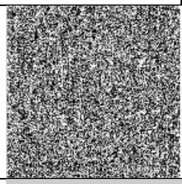
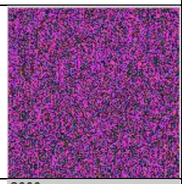
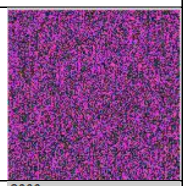
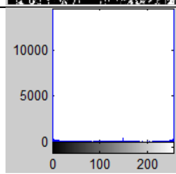
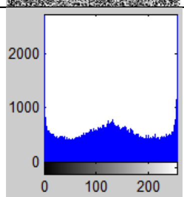
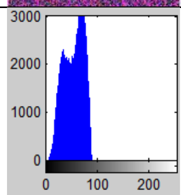
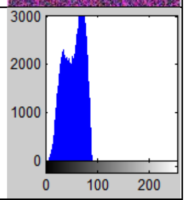
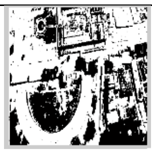
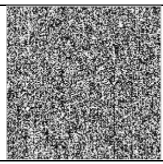
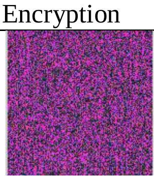
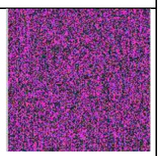
Tirumala area HSZ Data Encryption	Input Satellite Image	Gray Scale Image	Cubic Map Encryption	Logistic Map Encryption	Final Output Image
Image					
Histogram Equalization	NIL				

Table 5: Tirumala area of PPZ encryption with CMRSDE

Tirumala Temple PPZ Data Encry.	Input Satellite Image	Gray Scale Image	Cubic Map Encryption	Logistic Map Encryption	Final Output Image
Image					

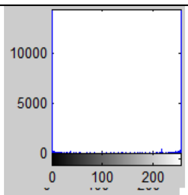
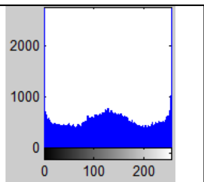
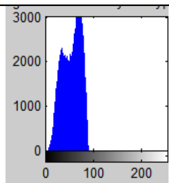
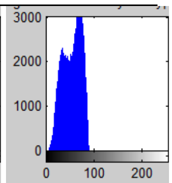
Histogram Equalization	NIL				

Table 6: Naval Dockyard area of HSZ encryption with CMRSDE

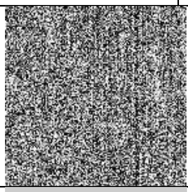
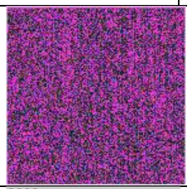
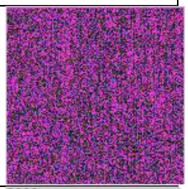
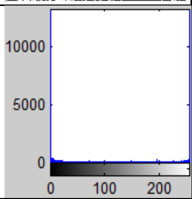
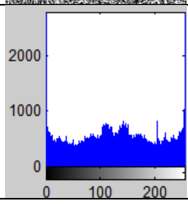
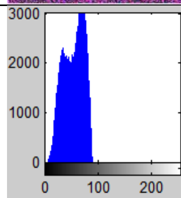
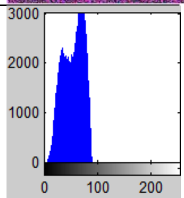
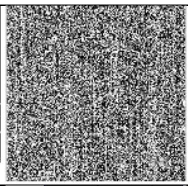
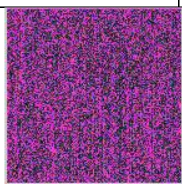
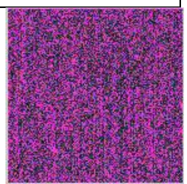
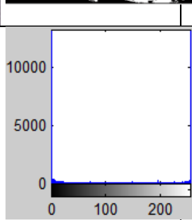
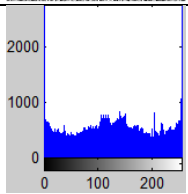
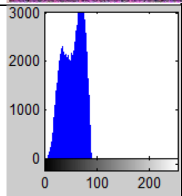
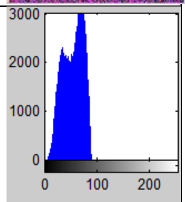
Naval Dockyard HSZ Data Encryption	Input Satellite Image	Gray Scale Image	Cubic Map Encryption	Logistic Map Encryption	Final Output Image
Image					
Histogram Equalization	NIL				

Table 7: Naval Dockyard area of PPZ encryption with CMRSDE

Naval Dockyard Ship sailing PPZ Data Encryption	Input Satellite Image	Gray Scale Image	Cubic Map Encryption	Logistic Map Encryption	Final Output Image
Image					
Histogram Equalization	NIL				

Impact of Computation time

Computation time is considered as one of the metric for CMRSDE encryption. The results were taken into consideration and computations were measured accordingly. Figure 2 shows different computation times of simulated data. But the computation time is too low for RSA algorithm [23] compared to CMRSDE, because CMRSDE is an double encrypted algorithm .

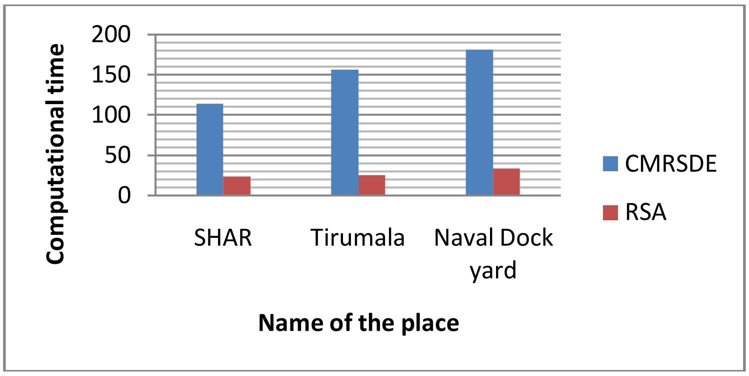


Figure 2: Impact of Computation time on RSI using Chaotic and non-Chaotic algorithm

Figure 3 compares the selective chaos based algorithm with non-selective chaos based algorithm. It is clearly observed that, Selective encryption on chaotic based algorithm performed well than rest. The computation is minimized in selective encryption.

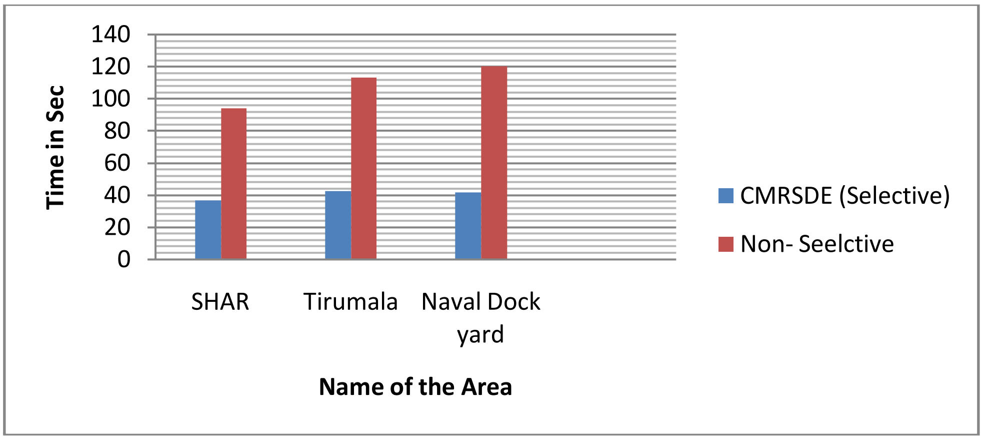


Figure 3: Impact of computation time of RSI data using Selective Chaotic and non-Selective Chaotic algorithm

Impact of Image data storage

When the data is stored of encrypted will take more space compared to non-encrypted image. The population is increased. The CMRSDE will occupy more data, due to its computation and population of pixels. If the computation is more the algorithm is stronger. Figure 4 the results of the data storage in KB. In this the CMRSDE occupied more data, compared to the RSA algorithm.

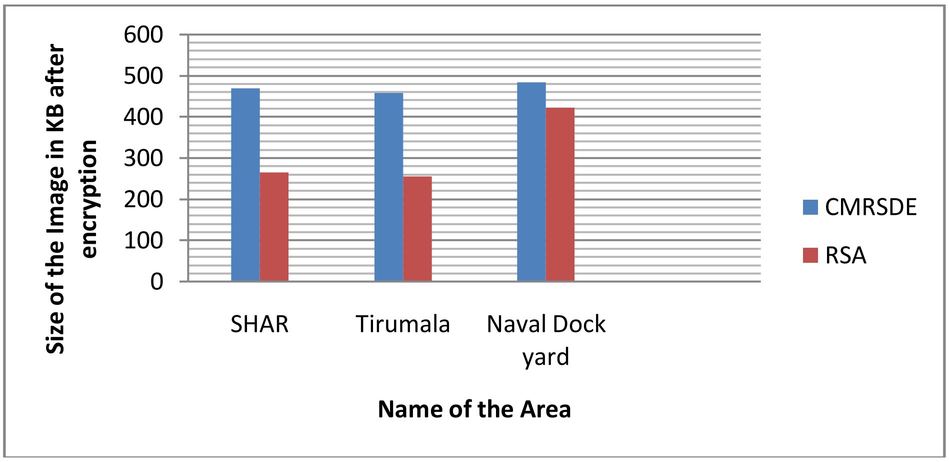


Figure 4: Impact of data storage on RSI using Chaotic and non-Chaotic algorithm

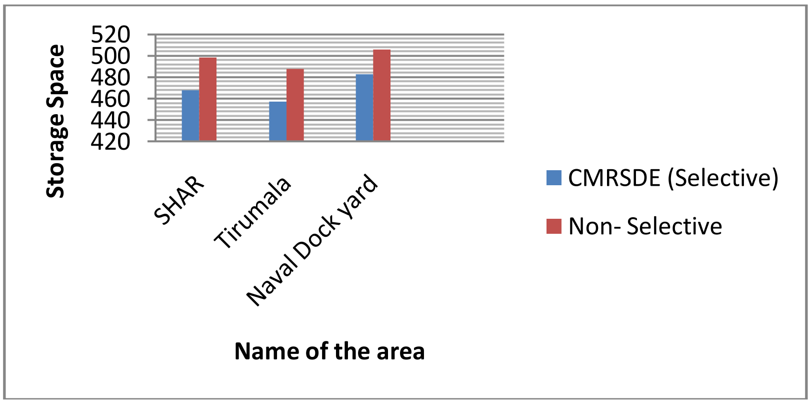


Figure 5: Impact of data storage on RSI using Selective Chaotic and non-Selective chaotic algorithm

Figure 5 compares the selective chaos based algorithm with non-selective chaos based algorithm. It is clearly observed that, CMRSDE consumes less data space than Non-selective encryption chaos based algorithm data storage space.

Overall Performance

The overall performance was calculated according to the equation 6. The overall performance is a combination of computation time and data storage. Overall performance is indirectly proportional to throughput. Figure6 represents the OP of the selective based and non-selective chaos based encryption. Besides assuring equal security the throughput of CMRSDE is good compared to Non-selective chaos based algorithm. Figure 7 explain the overall working procedure of CMRSDE.

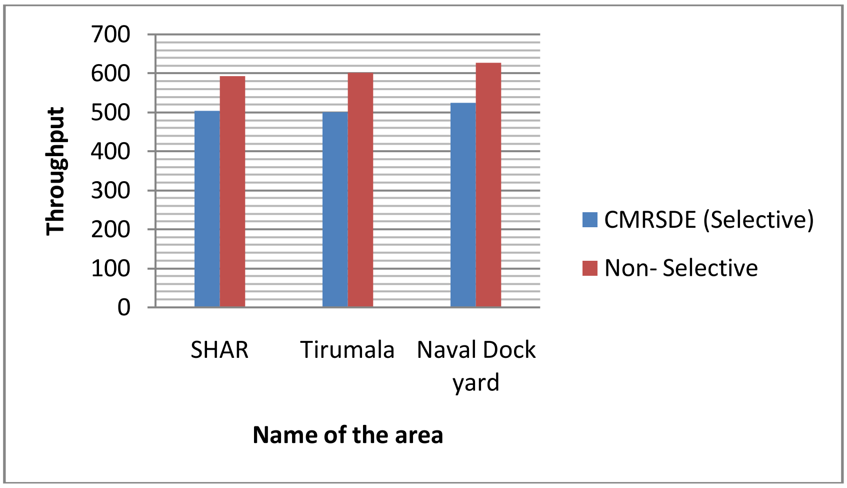


Figure 6: Overall performance on RSI using Selective Chaotic and non-Selective chaotic algorithm

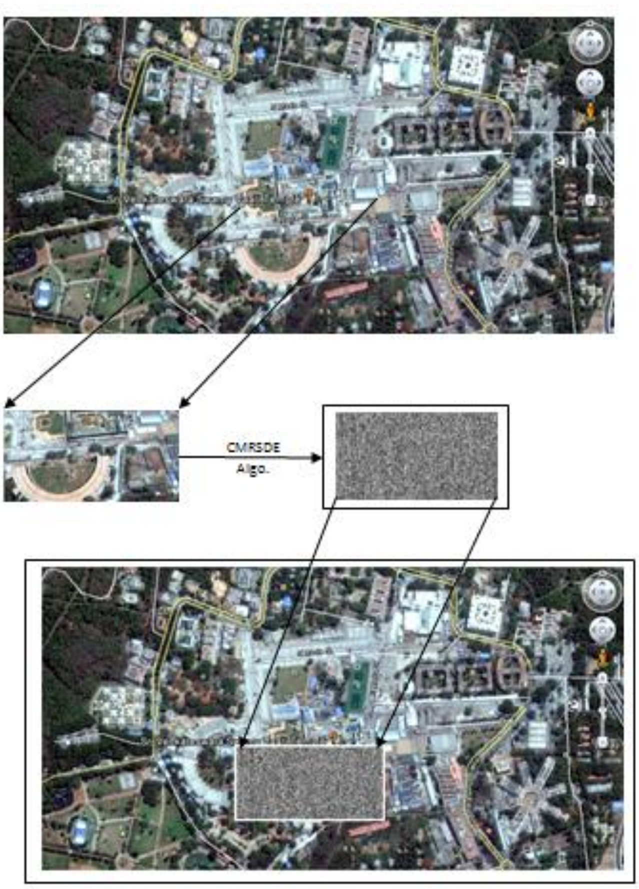


Figure 7: Overall Working procedure of CMRSDE

Conclusions and Future Scope

Global Terrorism is an challenging issue, where is whole world is thinking about. Terrorist groups are using RSI data as source for attacking on the HSZ in India and rest. In Oder to prevent the HSZ RSI data, many researchers discussed many chaos based techniques and non Chaos based techniques. This work introduces a novel selective based multi level encryption beside assuring the stronger security and reduction in the computation time, which resulted CMRSDE algorithm. The CMRSDE results were compared with non-chaos based algorithm and also Non-selective based chaos algorithm. It is observed that significant approximately 15% improvement of overall performance through computation reduction. Still there is scope further reduction in computation time of encrypted RSI data.

Reference

[1] http://en.wikipedia.org/wiki/2008_Mumbai_attacks (accessed on 01/12/2014)

[2] Pohl, Cle, and J. L. Van Genderen. "Review article multisensor image fusion in remote sensing: concepts, methods and applications." International journal of remote sensing 19.5 (1998): 823-854.

[3] Campbell, James B. Introduction to remote sensing. CRC Press, 2002.

[4] Hackwell, John A., et al. "LWIR/MWIR imaging hyperspectral sensor for airborne and ground-based remote sensing." SPIE's 1996 International Symposium on Optical Science, Engineering, and Instrumentation. International Society for Optics and Photonics, 1996.

[5] Biggar, Stuart F., Kurtis J. Thome, and Wit Wisniewski. "Vicarious radiometric calibration of EO-1 sensors by reference to high-reflectance ground targets." Geoscience and Remote Sensing, IEEE Transactions on 41.6 (2003): 1174-1179.

[6] Driggers, R., et al. "MWIR persistent surveillance performance for human and vehicle backtracking as a function of ground sample distance and revisit rate." SPIE Defense and Security Symposium. International Society for Optics and Photonics, 2008.

[7] Usama, Muhammad, et al. "Chaos-based secure satellite imagery cryptosystem." Computers & Mathematics with Applications 60.2 (2010): 326-337.

[8] Huang, Xiaoling. "Image encryption algorithm using chaotic Chebyshev generator." Nonlinear Dynamics 67, no. 4 (2012): 2411-2417.

[9] Muhaya, Fahad Bin, Muhammad Usama, and Muhammad Khurram Khan. "Modified AES using chaotic key generator for satellite imagery encryption." Emerging Intelligent Computing Technology and Applications. Springer Berlin Heidelberg, 2009. 1014-1024.

[10] Blaschke, Thomas. "Object based image analysis for remote sensing." ISPRS journal of photogrammetry and remote sensing 65.1 (2010): 2-16.

[11] http://landsat.usgs.gov/band_designations_landsat_satellites.php (accessed on 15/12/2014)
[12] Knight, Edward J., and Geir Kvaran. "Landsat-8 operational land imager design, characterization and performance." Remote Sensing 6.11 (2014): 10286-10305.
[13] Narayan, L. R. A. Remote sensing and its applications. Universities Press, 1999.
[14] Ganesh, L., and Sudhakar Godi. "Improved Security Levels of WLAN through DBSPS." International Journal of Computer Applications 106 (2014).
[15] Panduranga, H. T., and S. K. NaveenKumar. "Selective image encryption for Medical and Satellite Images." International Journal of Engineering and Technology (IJET) 5, no. 1 (2013): 115-121.
[16] Rajesh Duvvuru, Sunil Kumar Singh, K. Gowri Sankar and S. Deepthi. “Prediction And Analysis Of Bomb Blasts In India.” In Proc. of International Conference on Communication and Computing (ICC-2014), Elsevier, Banglore, India, 12-14 June 2014
[17] Pareek, Narendra K., Vinod Patidar, and Krishan K. Sud. "Image encryption using chaotic logistic map." Image and Vision Computing 24, no. 9 (2006): 926-934.
[18] Rogers, Thomas D., and David C. Whitley. "Chaos in the cubic mapping." Mathematical Modelling 4, no. 1 (1983): 9-25.
[19] Acharya, Anuja Kumar. "Image encryption using a new chaos based encryption algorithm." Proceedings of the 2011 International Conference on Communication, Computing & Security. ACM, 2011.
[20] Matsumoto, Makoto, and Takuji Nishimura. "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator." ACM Transactions on Modeling and Computer Simulation (TOMACS) 8.1 (1998): 3-30.
[21] Liu, Lijie, and Guoliang Fan. "A new JPEG2000 region-of-interest image coding method: partial significant bitplanes shift." Signal Processing Letters, IEEE 10.2 (2003): 35-38.
[22] Bascle, Kent P., et al. "Digital map generator and display system." U.S. Patent No. 5,140,532. 18 Aug. 1992.
[23] Alcorn, Allan E., and Richard L. Hale. "Method and apparatus using geographical position and universal time determination means to provide authenticated, secure, on-line communication between remote gaming locations." U.S. Patent No. 6,104,815. 15 Aug. 2000.
[24] Duvvuru, Rajesh, et al. "Scheme for Assigning Security Automatically for Real-Time Wireless Nodes via ARSA." Quality, Reliability, Security and Robustness in Heterogeneous Networks. Springer Berlin Heidelberg, 2013. 185-196.
[25] Duvvuru, Rajesh, P. Jagadeeswara Rao, and Sunil Kumar Singh. "Improvizing Security levels in WLAN via Novel BSPS." Emerging

Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA), 2013 International Conference on. IEEE, 2013.

[26] Duvvuru, Rajesh, P. Jagadeeswara Rao, Sunil Kumar Singh, and Ankita Sinha. "Enhanced Security levels of BSPS in WLAN." International Journal of Computer Applications 84, no. 2 (2013): 33-39.

[27] Duvvuru, Rajesh, et al. "Performance Analysis of Multi-class Steganographic Methods Based on Multi-Level Re-stegnography." ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II. Springer International Publishing, 2014.

[28] Wang, Fangju. "Fuzzy supervised classification of remote sensing images." Geoscience and Remote Sensing, Ieee Transactions On 28.2 (1990): 194-201.

[29] G. Narasimha Rao, R Ramesh, D Rajesh, D Chandra Sekhar. " An Automated Advanced Clustering Algorithm for Text Classification" Published in IJCST Vo l. 3, Issue-2, April-June,2012.784-787.

[30] G. Narasimha Rao , Rajesh Duvvuru, V.Chandrakala, B.Balakrishna . "A navie Clustering Algorithmfor Text Classification Based on feature vectors. " In Proc. of National Conference on Recent Trends in Computing and Information Technology NCRTC 2012; 55-59, July 2012