Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.743 – 750

SEGMENTATION AND ENCRYPTION OF SATELLITE IMAGES USING STREAM CIPHER ALGORITHM

P.Gunavathy
Final year
Department of ECE
IFET College of Engineering
gunavathy.parthiban@gamil.com

Mr. A.Vinoth Kannan, ME
Assistant Professor
Department of ECE
IFET college of Engineering
vinothkannana7@gmail.com

ABSTRACT: Information security plays one of the very important roles in the field of emergent information and communication technology. The applications such as medical images and satellite images needs the security only in the required portion, which contains the useful information .To improve the perception of surroundings and to monitor the earth's surface, remote sensing is used and it led the way for progress in information technologies. This paper explains the concept of enhancing the resolution of an image to improve the number of pixels, which is used to represent the details of an image and then segmenting the input image by using canny edge detector and encrypting the segmented image by using RC4 stream cipher algorithm. This encryption algorithm provides the security by XOR the plaintext and key. Moreover, RC4 algorithm (stream cipher) is considered to be providing a best result in terms of security, accuracy, noise, distortion less images by the varying features like variable key size and packet size.

Index terms: Segmentation, canny edge detection, encryption, cipher text, decryption.

SECTION I:

INTRODUCTION:

Due to the speedy improvement within the field data of knowledge and communication technology there is a good demand for information security. Generally, a picture is taken into account to be the two dimensional knowledge that carries a lot of information[1]. Remote sensing on broad satellites techniques is taken into account to be the foremost rising and powerful tools for the observation of the Earth's surface and atmosphere on a world, regional, and even native scale, and provides the importance on the sphere of agricultural, soils, etc and therefore the current state of the art of remote sensing processing within the image based mostly application fields [2-4].In this project, the satellite image is first increased by mistreatment bar graph exploit methodology so as to extend the resolution

and this can offers the entire details regarding picture element values of a picture. this can be a spatial domain based mostly improvement methodology and it'll enhance the image by mistreatment picture element by picture element. So, every and each pixels in a picture are often increased and it provides the method for extracting the mandatory options that is required for more process. to get the foreground image kind background image and to get the helpful info from the image, segmentation method is employed. The sting discover ion methodology is employed for this segmentation of satellite image as a result of it provides higher blessings cherish it will detect good outlines, less noise and orientation of image once comparison with alternative segmentation ways. This method detects outlines of associate object and limits between objects and therefore the background within the image. associate edge-detection filter also can be wont to improve the looks of blurred image and therefore the discontinuities at abrupt changes in picture element intensity that characterize boundaries of object. Cryptography is that the method of protective the knowledge by reworking it into associate undecipherable format within which a message are often hidden from the casual reader and solely the meant recipient are ready to convert it into original. Its main goal is to stay the information secure from unauthorized access [5]. the conventional knowledge which needs security is named plaintext or clear text. the tactic of disguising plaintext in such the simplest way on hide the knowledge is named encoding. Encrypting plaintext leads to undecipherable format is named cipher text. the method of reconverting cipher text to its original plaintext is named coding. within the existing methodology, block cipher formula is employed and in this paper, the encoding formula employed in this project is RC4 stream cipher formula, which can encrypts the stream of bits .The block cipher formula has 2 inconveniences, the primary one is that ,all blocks of this sort an encrypted on identical manner. The second downside was that block encoding ways don\'t seem to be strong to noise. to beat these disadvantages, stream cipher encoding formula is employed. This methodology is strong to moderate noise like JPEG compression with prime quality issue. The planned methodology incorporates the segmentation with encoding formula and it offers access to embedded security attributes within the encrypted domains for the aim of substantiative the dependability of a picture. The remainder of this paper is organized as follows: Section II proposes the connected works, Section III presents the planned work, Section IV presents simulation and experimental results, section V provides conclusions drawn from the findings of this work.

SECTION II:

RELATED WORKS:

Image segmentation is that the tactic of dividing an image into fully completely different components like sections, region and this methodology is acceptable for various applications, like automatic review [6].Gonzalez explains regarding the automatic review in electronic assemblies and it segments the image to hunt out defects, like a missing or broken path [7]. information is hidden among completely different file formats like text, image, audio/image, and this protocol is tired a pair of ways that within which like spatial domain and frequency domain[8] . Prasanna et al. projected the part manipulation and secret writing for the medical footage, it explains with one dimensional distinct Fourier retread for secret writing purpose and private key cryptosystem for secret writing, and this methodology works inside the frequency domain[9]. Ju-Young American state, Dong-Il principle, Ki-Hwan Chon, 2010 [10] projected a system to expand the advanced secret writing commonplace (AES)-Rijndael with five criteria: the first is that the compression of plain knowledge, the second is that the variable block size , the third is that the selectable spherical for key generation, the fourth is that the optimization of code implementation and conjointly the fifth is that the selective performance of the complete routine. Gautam and Dr.P.R Gupta projected the simplest way where they used the block based mostly cipher for secret writing methodology which they got the output that takes superabundant times, though it produces the various result. but complexities for the block cipher is massive and all over again execution time is kind of high[11]. Dalel Bouslimi et al projected that, new joint watermarking/ secret orthography, that guarantees a priori and a posteriori protection of medical footage. It merges the QIM and a cipher algorithmic rule or a block cipher algorithmic rule. But, the disadvantage inside the methodology is that, the tactic could be a heap of advanced and conjointly the cryptography is subtle and it is a heap of attack on the JPEG images[12]. Parameshachari B. D et al[13], projected that a totally distinctive conception of component price manipulation practice half manipulation in frequency domain and sign secret writing for partial secret writing methodology. 9It incorporates a heap of applied mathematics attacks on the cipher text and conjointly the PSNR worth obtained could be a smaller quantity. But, collectively it achieves the foremost effective security by higher correlation and entropy. Vinay pandey et al [14] projected a combined approach practice cryptography, data concealing and steganography. throughout this technique ,the original image is encrypted practice stream cipher methodology therefore the encrypted image is embedded practice lossless data concealing methodology with patient information. Inside the receiver aspect, reversible data concealing algorithmic rule is applied on the encrypted image

to urge eliminate the embedded data before image cryptography. so as that we tend to discover tons of secured and denoised medical image. Quist-Aphetsi Kester, counseled the key writing technique, that depends on component shuffling and it generates a secret key, that produces the cipher text with no component enlargement . But, the matter throughout this technique is that, a little modification inside the ciphered image size will results in the modification in cryptography result and conjointly the typical total component before secret writing was the same as a result of the typical total component once encryption[15]. Jitendra leader et al [16] projected the general algorithmic rule for partitioning grayscale footage into disjoint regions of coherent brightness and texture. Natural footage contain every le and non-textured regions, that the contour and texture variations unit exploited at identical time

SECTION III:

PROPOSED WORK:

The idea of planned methodology is explained by the diagram. The diagram is explained as follows

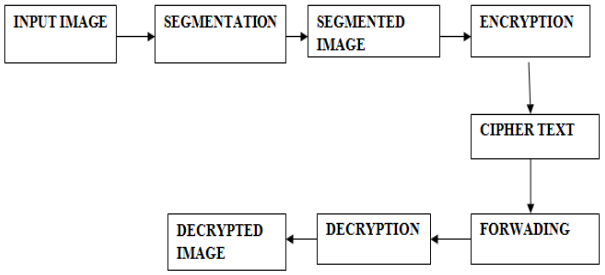

Fig1:Block diagram of proposed work

A.INPUT IMAGE:

Within the planned technique, the input image is that the image captured by the satellite. This image is increased i.e. distinction improvement is finished so as to extend the resolution of the pixels of a picture. bar graph equalization is employed for the distinction improvement, that may be a spatial domain transformation methodology. This may transforms every and each pixels of a picture therefore, the options is simply extracted from the image.

B.SEGMENTATION:

Segmentation is employed to separate the regions that square measure visually dissimilar, uniform and significant with relevancy some characteristics or property like grey level, texture or color that paved the method for straightforward image analysis. Segmentation is that the method of partitioning a picture into multiple segments and to extract the significant info i.e. Region of Interest (ROI) from a picture.

Segmentation techniques is categorized into 2 broader approaches:

1. Boundary –based or edge based mostly strategies

2. Region based mostly strategies

The first approach relies on separation and tends to partition a picture by detective work isolated points, lines and edges in keeping with abrupt changes and native properties. The regions square measure then deduced from their boundary. The second approach includes thresholding , clustering, region growing, region cacophonic and merging that exploit the homogeneity of data like intensity, color, texture properties ,etc,. to provide the segmental results. Within the planned technique, edge based mostly segmentation methodology is employed. Edge plays a really vital role in several image process applications, as a result of it provides define of the item. A foothold may be a set of connected pixels that lies on the boundary between 2 regions that dissent in gray price.

EDGE DETECTION TECHNIQUES:

These pixels on the sting square measure referred to as edge points. a foothold is often extracted by computing the spinoff of the image operate. The categories of edge detection techniques are:

- First order derivative
- Second order derivative

STEPS IN EDGE DETECTION:

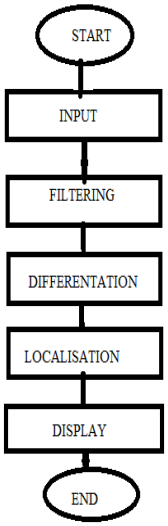

Fig 2: Process of canny edge detection

FIRST ORDER DERIVATIVES:

ROBERT OPERATOR:

The Roberts Cross operator performs an easy, fast to reckon the 2-D spacial gradient activity on a picture. Element values at every purpose within the output represent absolutely the magnitude values of spacial gradient of the input image at that time.
The gradient magnitude important is given as,
$|G| = \sqrt{Gx^2} + \sqrt{Gy^2}$
The approximated magnitude is given as,
$|G| = |Gx| + |Gy|$

PREWITT OPERATOR:
It is used for detective work horizontal and vertical edges in a picture.

SOBEL OPERATOR:
This operator is meant to sight the perimeters running vertically and horizontally in accordance to the element values for every of the 2 perpendicular orientations. It is applied one by one to the input image, to provide separate measurements of the gradient part in every orientation of a picture.
The gradient magnitude is given as,
$|\Delta f| = \sqrt{Gx^2} + \sqrt{Gy^2}$
The approximated magnitude is given as,
$|\Delta f| = |G_x| + |G_y|$

The disadvantages of initial order derivatives square measure it's additional sensitive noise, it manufacture thick edges and also the inaccurate edges of associate degree pictures square measure determined. To overcome the disadvantages of initial order derivatives, second order spinoff is employed.

SECOND ORDER DERIVATIVE:

The Laplacian may be a 2-D identical live of the 2D spatial spinoff of a picture. It highlights the regions of fast intensity variation and is thus typically used for edge detection. The Laplacian is applied to mathematician Smoothing filter so as to smoothen the image ,which is employed for cut back the sensitivity to noise. The operator usually takes one grey level image as input and produces another grey level image as output.

The Laplacian L(x,y) of a picture with element intensity values I(x,y) is given by:

$$L(x,y)=\partial^2 I/\partial X^2+\partial^2 I/\partial y^2$$

The disadvantages of second order spinoff square measure, it's unable to search out the orientation of the photographs.

CANNY EDGE DETECTION:

Canny edge detection technique is incredibly necessary methodology notice to seek edges by analytic noise from the image before find edges of image, while not poignant the options of the perimeters within the image then applying the tendency to search out the perimeters and also the important price for threshold. This methodology has additional blessings over different strategies in such some way that, it will sight solely true edges and discard all the opposite false edges. In cagy edge detector, the input image is filtered by victimisation mathematician filter. So, it will manufacture skinny edge and amplitude is suppressed in a picture. The gradient is calculated for the filtered image and also the edge magnitude and orientation of the gradient square measure hold on in 2 separate arrays. It uses 3 criteria's for good segmentation. The primary criteria is that, it manufacture low error rate. The second criterion is that the sting points be localized. The third criterion is to own just one response to one edge.

ALGORITHM FOR CANNY EDGE DETECTION:

The recursive steps for cagy edge detection technique square measure follows:

1.Twist image f(r, c) with a mathematician operate to urge sleek image f^(r, c).

f^(r, c)=f(r,c)*G(r,c,6)

2. Apply initial distinction gradient operator to reckon edge strength then edge magnitude and direction square measure acquire as before.

3. Apply non-maximal or important suppression to the gradient magnitude.

4. Apply threshold to the non-maximal suppression image.

The benefits cagy edge detection square measure, has the characteristics of each initial order and second order derivatives, produces good contours, low error rate and has single edge purpose response.

C.ENCRYPTION:

The cryptography algorithmic rule employed in this planned idea may be a RC4 stream cipher . RC4 may be a cipher made-up by Ron Riverst. This algorithmic rule is additionally referred to as Riverst cipher four algorithmic rule. RC4 is most well liked encoding algorithmic rule , it's employed in variety of Wired Equivalent Privacy (WEP) employed by IEEE 802.11x normal in Wireless local area network. it's a symmetrical stream cipher algorithmic rule, that generate a pseudorandom stream of bits as a key. The stream cipher algorithmic rule combines the plaintext by finding the two modulus addition of the key stream and also the plaintext. RC4 is straightforward and imposingly quick. it's a cipher of up to 256bytes key size and creates a stream of random bytes and Xoring those bytes with the text. The key repetition ought to be avoided during this methodology to produce the image higher security. The XOR operation is applied to pseudorandom noise generator withT = [t1, . . . ti, . . . , American state] with a secret key stream of bits/bytes K = [k1, . . . ki, . . . , kn] The stream cipher becomes a neighborhood of symmetrical key as a result of the key generation depends upon the key key Ke. Thus, bits/bytes of cipher text C = [c1, . . . ci, . . . , cn] square measure typically outlined as ci = ti XOR ki . a number of the most blessings of this kind of algorithms square measure that they're easy and operate at a better speed than block cipher algorithms [13]. The specificity of such stream cipher algorithmic rule is that the key generation by victimisation the pseudo random noise generator (PRNG).

The RC4 PRNG relies on 2 steps.

1) "Initialization," wherever a table of 256 bytes is stuffed by repetition the cryptography key as typically as necessary.

2) "Byte key stream generation," wherever the weather of the square measure combined by applying permutations and additions to get the key stream.

This type of attacks occurs when hacker temporally gains access to the decryption machine carefully hacker select some cipher texts send them through the machine to obtain the corresponding plaintexts. Now hacker can do a known plaintext attacks and again if, he select his cipher text messages correctly hacker would have an easier time to finding the key. Cryptographic methods have their own strengths and weaknesses and these are depends upon the requirement.

MODEL OF STREAM CIPHER ALGORITHM:

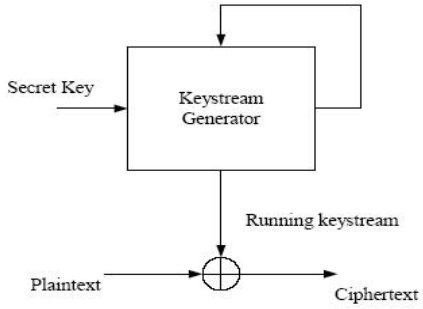

Fig 3. Model of stream cipher algorithm

D.DECRYPTION:

RC4 algorithmic rule may be a symmetrical key algorithmic rule, during which each the sender and receiver uses identical key. The key generated from the cryptography block is passed towards the receiver aspect. So, by victimization the receiver rewrite the image to urge the first image. The cryptography and secret writing method of RC4 stream cipher cryptography algorithmic rule is given as,

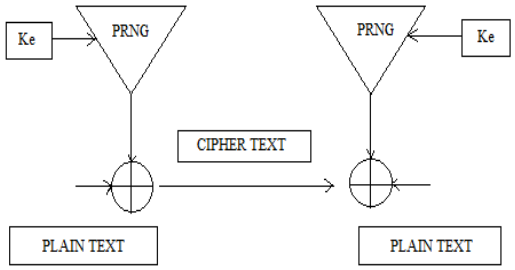

Fig 4. Encryption and decryption of stream cipher algorithm

SECTION IV:

SIMULATION AND EXPERIMENTAL RESULTS:

These figures 5, 6 and 7 are the square measure generated when simulation victimization MATLAB and these totally different figures have different characteristics. Figure 5 represents the input image and the enhanced image is obtained by the preprocessing, to make the image suitable for further applications.

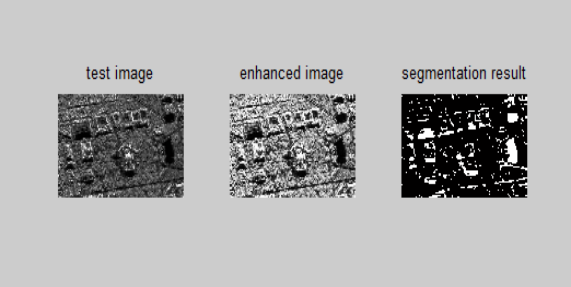

Fig 5: input and segmental image

Fig 6: encrypted image

Fig 7: decrypted image

SECTION V:

CONCLUSION:

During this paper we tend to bestowed a 2 selective method for image cryptography approach for satellite pictures. Initial approach is segmenting the image by victimization cagy edge detector. It'll manufacture good define, noise free and excellent orientation of the image. The segmentation method is applied square measure terribly helpful once the world or region of interest is understood. Second approach is that the cryptography method. RC4 cryptography can encrypts the stream of bits and also the key size are additional and also the pseudo random noise generator can manufacture the random sequence of bits. So, it provides further security. Thus, these 2 approaches square measure greatly appropriate for specific applications square measure satellite image cryptography.

REFERENCES:

[1] Simone, G.; Farina, A.; Morabito, F.C.; Serpico, S.B; Bruzzone, L. .,2002. "Image fusion techniques for remote sensing applications". Inf. Fusion 2002, 3, 3–15.
[2] Myint, S.W., Yuan, M., Cerveny, R.S., Giri, C.P., 2008. Comparison of remote sensing image process techniques to spot tornado harm areas from landsat metallic element knowledge. Sensors eight (2), pp.1128-1156.
[3] T. Blaschke, 2010. "Object based mostly image analysis for remote sensing". Review Springer, ISPRS Journal of Photogrammetry and Remote Sensing sixty five (2010) ,PP. 2-16.
[4] Kai Wang, Steven E. Franklin , Xulin Guo, brandy Cattet ,2010. "Remote Sensing of Ecology, multifariousness and Conservation: A Review from the angle of Remote Sensing Specialists". critique, Sensors 2010, 10, 9647-9667; doi:10.3390/s101109647
[5] Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed, "Evaluating the Performance of symmetrical cryptography Algorithms" International Journal of Network Security, Vol.10, No.3,pp.213- 219, May 2010.
[6] "A Joint Encryption/Watermarking System for validatory the responsibleness of Medical Images", IEEE TRANSACTIONS ON info TECHNOLOGY IN BIOMEDICINE, VOL. 16, NO. 5, Sept 2012.
[7] T. Morkel, J.H.P. Eloff, and M.S. Olivier, "An summary of Image Steganography," Proceedings of the Fifth Annual info Security South Africa|African country|African nation} Conference. (ISSA2005), Sandton, South Africa, June/July 2005. (Published electronically)
[8] Prasanna SRM et al, 2009, "An image cryptography methodology with magnitude and part manipulation victimisation carrier images", IJCS 1(2):132–137.
[9] Ju-Young American state, Dong-Il rule, Ki-Hwan Chon, 2010, "A Selective cryptography algorithmic rule supported AES for Medical Information", the Korean Society of Medical Informatic
[10] R. C. Gonzalez, and R. E. Woods. Digital Image Processing. higher Saddle River: Prentice-Hall, 2012
Advanced Engineering, Volume 2, Issue 1, January 2011)
[11] "Secure Transmission of a picture victimization Partial cryptography based mostly algorithmic rule" International Journal of pc Applications (0975 – 8887) Volume 63– No.16, Feb 2013
[12] "Medical Image Protection by victimization Cryptography Data-Hiding and Steganography" International Journal of rising Technology and
[13] "A visual cryptological cryptography technique of securing medical images", International Journal of rising Technology and Advanced Engineering Volume three, Issue 6, June (2013)
[14] "Contour and Texture Analysis for Image Segmentation" International of rising technology and advanced Engineering,volume1,Issue1,november2013

