ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8 , August 2017

A Novel Approach For Image Security

[1] Jyoti T. G. Kankonkar, [2] Nitesh Naik
[1][2] Department of Computer Engineering, Goa College Of Engineering, Goa

***Abstract*— Image security is a major concern as the digital communication and digital data is growing rapidly. Image data is generated in loads every day. We need faster and robust mechanisms to secure the image data. Various fields such as military scopes, security firms, social network etc. need systems that can protect the images while communicating and data transfers. In this paper the proposed idea involves use of image encryption using chaotic approach with a combination of image stitching mechanism. This unique combination provides double layered protection to the images. In order to transfer an image, the image is first partitioned, encrypted and then transferred making it difficult for attackers to access the whole image. On the other end, the encrypted image is decrypted using a symmetric key generated using chaotic approach that uses logistic map function and linear feedback shift register which is followed by image stitching procedure..**

***Keywords*— Image encryption, Image stitching, Logistic Map function, Linear feedback shift register.**

INTRODUCTION

The security of digital images has becomes an important issue with the rapid growth of digital communication and multimedia applications since the communication of digital products through networks occur frequently. As the cybercrimes are increasing, providing only network security is not sufficient. Secret images in military fields, security firms are more vulnerable to attacks. Encryption is used in most of the fields to ensure security. The image to be transferred is broken down into parts, encrypted using chaotic approach and transferred to the receiver. This makes it difficult for the attacker to get access to all the parts of the images at once. Thus increasing the security to a much needed higher level. This makes it highly difficult for the intruder to access all the partial images and decrypt them to have the original image.
Images are converted to a form which is difficult to understand thus providing image security and confidentiality against attacks. It is expected that the wrong key will generate an incorrect outcome and nobody will be able to access the data without the correct key. Most of the encryption algorithms used are more suitable for textual data and not multimedia data. Hence there is need for novel approaches that can provide security to the multimedia data such as image data and videos etc.

II. LITERATURE SURVEY

The paper [1] employed a new approach for image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of linear feedback shift registered. The two steps included were creation of an encryption key and using that key for image encryption. Firstly a logistic map function was used to generate highly random sequence K1 and an 8 bit linear feedback shift register to get a sequence K2.The key sequence used for encryption was generated using both K1 and K2. The key sequence generated was used with the pixel values obtained to get the encrypted image. Encrypted image when decrypted using the correct key generates the original image. It is observed that proposed encryption provides cryptographically better results than encryption using logistic map scheme and provides more security, secrecy to the image.

The paper [3] used a new image encryption scheme which employs one of the three dynamic chaotic systems (Lorenz or Chen or LU chaotic system selected based on 16-byte key) to shuffle the position of the image pixels (pixel position permutation) and uses another one of the same three chaotic maps to confuse the relationship between the cipher image and the plain-image (pixel value diffusion), thereby significantly increasing the resistance to attack.

The paper [2] proposed a symmetric color image encryption scheme with permutation-diffusion architecture. In the permutation stage, the three color components of a color image are shuffled separately by using Arnold cat map with the purpose of eliminating the strong correlation among adjacent pixels. Then in the diffusion process, the shuffled R, G, B components are masked by three pseudo-randomness key streams quantified from Chen's chaotic system, respectively, so as to confuse the relationship between the cipher image and plain image.

The paper [5] reviewed all the recent approaches proposed to perform the image stitching process. The main steps of image stitching are calibration, registration and Blending. Calibration aims to minimize differences between an ideal lens model and the camera-lens

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

combination that was used. The differences could be some optical differences. Image registration defined as the process of aligning two or more images which are captured from different point of perspective. Blending is applied across the stitch so that the stitching would be seamless.

The paper [4] reviewed an image stitching model which consists of: Image acquisition- Image acquisition is the process of retrieving an image from some sources. Feature detection and matching- The basic idea to do feature detection is that, the image can't be seen as whole an image but the special points in the image can be taken separately and then processed by applying feature detection methods feature matching of image pairs, corners are sufficiently matched. Image Matching- After performing feature detection, this information is used for image matching of all pictures. The main step of image matching is to find out that which pixel is a neighbour of another pixel, and find the correctly feature matching set for that image. Global Alignment- Global alignment is done to minimize the miss-registration between all sets of images. Blending and composition- The final step to stitch two images is to blend these images together. In blending, firstly a compositing surface is chosen, e.g., flat, cylindrical etc. and then decide how to blend these images to form an attractive panorama. For fewer image stitching, a natural approach is adopted in which one image is select as reference and then all other images are warp according to reference coordinate system.

The paper [6] studied high resolution image stitching problems on Open CV environment with various kinds of Harris image stitching algorithms. The Harris corner detection algorithm was used to extract the feature points. Normalized Cross Correlation was used to rough match the feature points and RANSAC algorithm was used to eliminate error matching. For image registration algorithm, cylindrical projection transformation model was used. An improved weighting average fusion algorithm was used to fuse images and to reduce the computational complexity of image fusion and to generate seamlessly stitched image.

III. PROPOSED WORK

The proposed technique uses both image encryption and image stitching to achieve security goals. Initially the image to be transferred is first partitioned into desired parts (considered 4 parts).

As the number of partitions of an image increases the security level is also increased. It is preferred based on the size of the image and the level of privacy of that image
The system is divided into two parts Sender's End and Receiver's End.

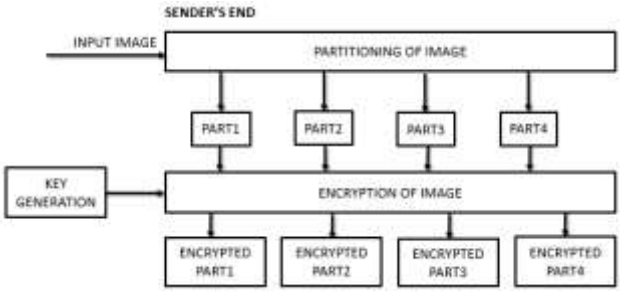

Fig. 1. Sender's End

Various phases in Sender's side are:
Fig. 31. Shows the Sender's End and how the data flows through various modules on the sender's end.

Partitioning of the image
While transferring an image the sender partitions the image into 4 parts. To crop the image into four parts the image height and width is calculated first and then based on the amount of overlapping required amongst the parts of the image, the image is cropped accordingly.

Key Generation
Key generation module uses two main functions namely logistic map function and linear feedback shift register. This two functions are used to generate two key sequences that generate the final key sequence to be used to encrypt the image. Logistic map function involves use of bifurcation parameter 'r'. The choice of 'r' decides the randomness, unpredictability in the key sequence generated. Basically, 'r' ranges from (0-4) and X0 is the initial value ranging from 0<X0<1 and the initial seed vale to be used in linear feedback shift register will be an 8 bit binary input. The key generation module is shown in Fig 3. The values r and X0 are given to function:

$$Xn+1 = r\ Xn\ (1 - Xn)$$

which generates K1 sequence and initial seed is given to an 8-bit Linear Feedback Shift Register which generates K2 sequence. The final is generated by calculating Key (i) = K1 (i) XOR K2 (i) where I goes till n where n is the number of pixels in the image.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

Encryption

The encryption procedure involves use of key sequence along with the image pixel values to manipulate them to generate the encrypted form of the image. Here for each of the pixels in the image, pixel values of the image and the key sequence are given to XOR function to generate encrypted image.

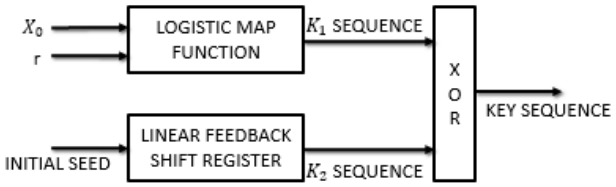

Fig. 2. Key Generation Module

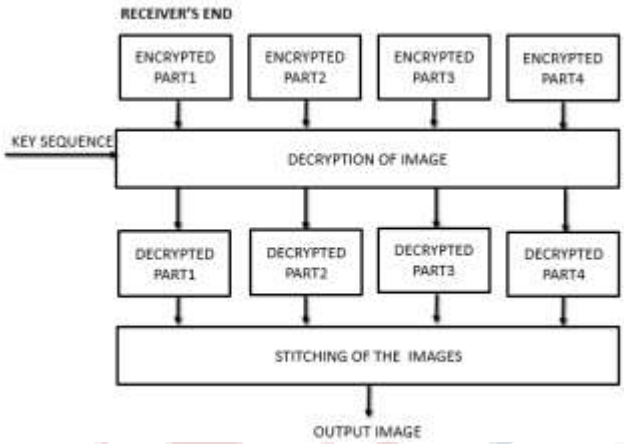

Fig. 3. Receiver's End

Various phases in Receiver's side are:
Fig. 3. Shows the Receiver's End and how the data flows through various modules on the receiver's end.

Decryption

The decryption procedure involves use of key sequence along with the encrypted image pixel values to manipulate them to generate the decrypted form of the Image. Note that for a wrong key sequence an incorrect image will be generated. Here for each of the pixels in the encrypted image, pixel values of the image and the key sequence are given to XOR function to generate decrypted image.

Image Stitching

The image stitching procedure involves use of set of decrypted images that are processed by the various procedures such as feature extraction, feature matching etc. to generate the original form of the Image. The overall image stitching procedure is shown in Fig 4. Feature Extraction, Feature Matching, Homography matrix estimation, RANSAC, Blending algorithms are performed on all the decrypted images to generate the stitched image.

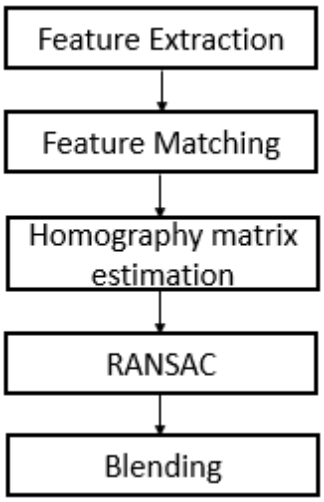

Fig. 4. Image stitching module

IV. EXPERIMENTAL RESULTS

This section of the paper discusses about the experimental results. Fig. 5. Shows the original image (left) and the image after applying partitioning algorithm.

Fig. 5. Image to be transferred (left), overlapping parttions of the image (right)

Fig. 6. shows the BGR (Blue, Green, Red) components of a partition 1 after encryption (left) and all the partitions shown in fig. 5. after applying encryption algorithm(right). En1, En2, En3, En4 are the partitions after encryption.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

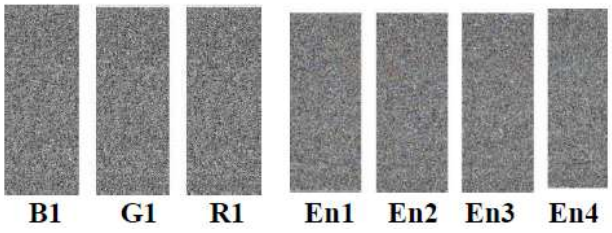

Fig. 6. BGR components of part1 after encryption (left), each of the encrypted parts (right)

Fig. 7. shows all the 4 partitions after applying decryption algorithm (left) and how the image looks after applying image stitching algorithm (right)

Fig. 7. Decrypted Parts of the image (left), image after image stitching

Fig. 8. shows the histogram for the original image and histogram for decrypted image. Both of the histograms looks similar.

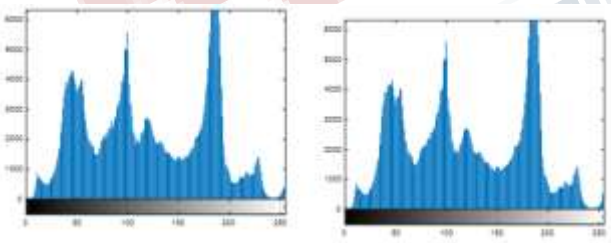

Fig. 8. Histogram for Original Image and Decrypted Image

Fig. 9. Shows the histogram for Blue, Green, Red components of the original image partition 1. Fig. 10. Shows Blue, Green, Red components of encrypted image partition 1 which is uniform in nature. Fig. 11. Shows histogram for Blue, Green, Red components of decrypted image partition 1 which is similar to histogram output of the original image partition 1 as shown in fig. 9.

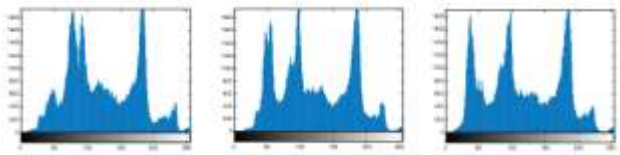

Fig. 9. Histogram for Blue, Green, Red components of Original Image Partition1

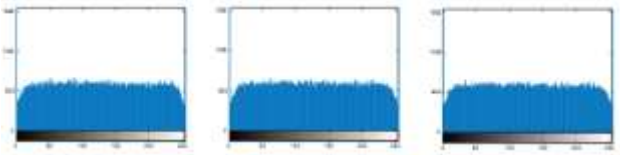

Fig. 10. Histogram for Blue, Green, Red components of Encrypted Image Partition1

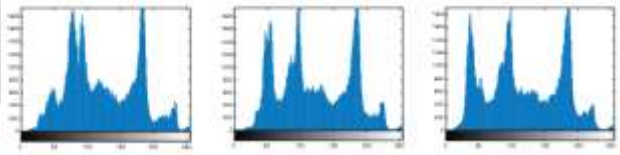

Fig. 11. Histogram for Blue, Green, Red components of Decrypted Image1

V. CONCLUSION

This paper proposes a system that consists of a combination of image encryption and image stitching techniques for image security. This unique combination provide a double layered protection to the images that are being transferred. The image encryption technique used is chaotic key sequence generated using the sequence generated by logistic map and sequence generated by states of linear feedback shift register. Image stitching using feature– based technique is used for performing image stitching on the multiple decrypted image parts. Use of chaotic approach makes it computationally faster and is more sensitive to the initial conditions making it difficult for attackers. Randomly generated keys makes it more unpredictable hence achieving the security goals of the system. The paper also shows the various experimental results and histogram outputs for a sample image.

REFERENCES

[1] Rohith S, K N Hari Bhat , A Nandini Sharma, ”

Image Encryption and Decryption using Chaotic Key Sequence Generated by Sequence of Logistic Map and Sequence of States of Linear Feedback Shift ", in 2014 International Conference on Advances in Electronics, Computers and Communications (ICAECC)

[2] Chong Fu, Jiaqi Tang1, Wei Zhou, Wenqi Liu, Dongliang Wang, " A Symmetric Color Image Encryption Scheme Based on Chaotic Maps", in 2013 15th IEEE International Conference on Communication Technology, Guilin, China

[3] K. Sakthidasan , B. V. Santhosh Krishna," A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images ", in International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011

[4] Shikha Arya," A Review on Image Stitching and its Different Methods", in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015

[5] Pranoti Kale, K.R.Singh," A Technical Analysis of Image Stitching Algorithm", in International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 284-288

[6] Chen Kaili, Wang Meiling," Image Stitching Algorithm Research Based on OpenCV " , Proceedings of the 33rd Chinese Control Conference July 28-30, 2014, Nanjing, China

[7] Derek Hoiem," Image Stitching", in Computational Photography, University of Illinois [ppt]

[8] Jyotika Kapur, Akshay. J. Baregar," Security using image processing", in International Journal of Managing Information Technology (IJMIT) Vol.5, No.2, May 2013

[9] Rahul Kumar, Ajit Pratap Singh, Arun Kumar Shukla, Rishabh Shukla," Enhancing Security Using Image Processing", in International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 4, April 2015

[10] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya," A Survey On Different Image Encryption and Decryption Techniques" in International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013