Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Keyless approach to Lossless Image Encryption

.Pratibha S. Ghode, IV SEM, M.Tech – CSE AbhaGaikwad-Patil College of Engineering, Nagpur, India.
[1] Prof. Pragati Patil Assistant Professor ,AbhaGaikwad-Patil College of Engineering,Nagpur, India.
[2]Prof.Vinod Nayyar Assistant Professor ,AbhaGaikwad-Patil College of Engineering,Nagpur, India.
[3]Prof.Shashank Moghe Team Lead, Persistant System Ltd,Nagpur, India.

Abstract: Some limitation of Key oriented techniques, to maintain the key records and increase high computational cost. This paper proposes an improved Keyless approach for image Encryption in lossless RGB images. There are three different approaches being followed in image encryption, the first approach to key oriented encryption and second approach to Image splitting and the last approach multiple share. The objective of this work is to increase the security level and to improve the storage capacity with SST techniques. The security level is increased by randomly distributing the pixel bit over the entire image. In this keyless approach to reversible encryption will be done and to maintain the originality of an image without any loss of quality.

Keywords: lossless image encryption, reversible encryption, transformation.

I. INTRODUCTION

Encryption is the process of encoding messages or information in such a method to only authorized party is able to read it. Encryption doesn't stop hacking but it reduces the possibility to the hacker resolve be able to read the data to is encrypted. Into an encryption system, the message or information, referred to as plaintext, be encrypted by means of an encryption algorithm, turning it into an illegible cipher text. This is typically done with the use of an encryption key, which specifies how the message be encoded. Any challenger that can observe the cipher text should not be capable to determine everything about the original message. An authoritative party, though, is able to decode the cipher text by decryption algorithms, which typically require a secret decryption key, which adversary achieve not have access to. For practical reasons, an encryption system usually wants a key-generation algorithm to at random produce keys [11].

Image encryption [12] is a process in which plaintext image is converted into cipher text so that it cannot be read. Additional usually known as "encryption," this process can be able into a wide variety of behaviour, and through varying degrees of achievement. Some of the best image encryption can last for centuries, whereas other types of decryption are able to be broken in minutes or even seconds with people who are skilled at such tasks. In the digital era, people rely greatly on image encryption resting on an everyday base. Chances are high to you have received or else sent encrypted data at a few point at the moment, even if you did not straight achieve the encryption or decryption of the image.

1.2 Digital Image and Bitmap

A digital image [10] is composed of pixels (short for picture elements). Every one pixel are represents the color (or gray level for black or white photos) by a single point in the image, so a pixel is similar to a tiny dot of a particular color. Through measure the color of an image next to a large numbers of points, we can create a digital estimate of image from which a copy of the unique can be reconstructed. Pixels are a little like granule particle in a predictable pictorial image, but arranged in a regular model of rows and columns and store information rather in a different way. A digital image is a rectangle array of pixels is known as bitmap.

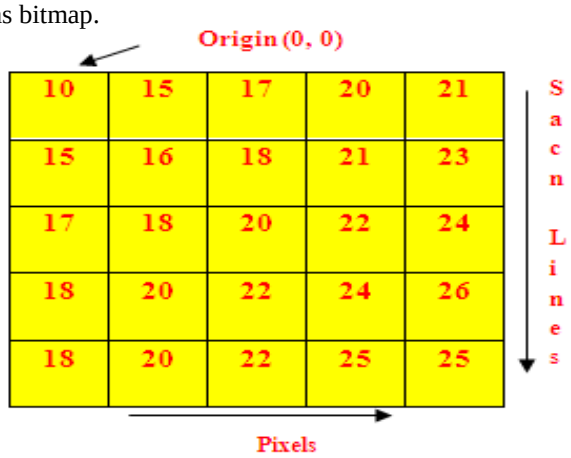

Fig: 1.1 Structure of Digital Image

Digital image processing is use of computer algorithm to do image processing on digital images. Since a digital processing filed has many reward over the analog image processing. It allow a much wider range of algorithm to be useful to the input data and can avoid problems such as the increase of noise and signal alteration during processing. Because images are defined over two dimensions (perhaps more) digital image processing may be modelled in the form of multidimensional systems.

II. RELATED WORK

2.1. Multiple Shares

A new method which performs, "A keyless approach to image encryption" to splitting an image into multiple shares proposed Siddharth Malik and Anjali Sardana [1]. In this encryption is based on SDS algorithm. SDS means Sieving, Division, and Shuffling. In the first step sieving technique generates the secret image is split into RGB colors. In the second steps Division technique generates the split images are randomly divided. In the three steps shuffling technique shuffled each shares and finally combined all shares.

2.1.1 Sieving

Sieving is process to filter the combined RGB components into individual R, G and B components .To make the process computationally inexpensive, and sieving uses the XOR operator.

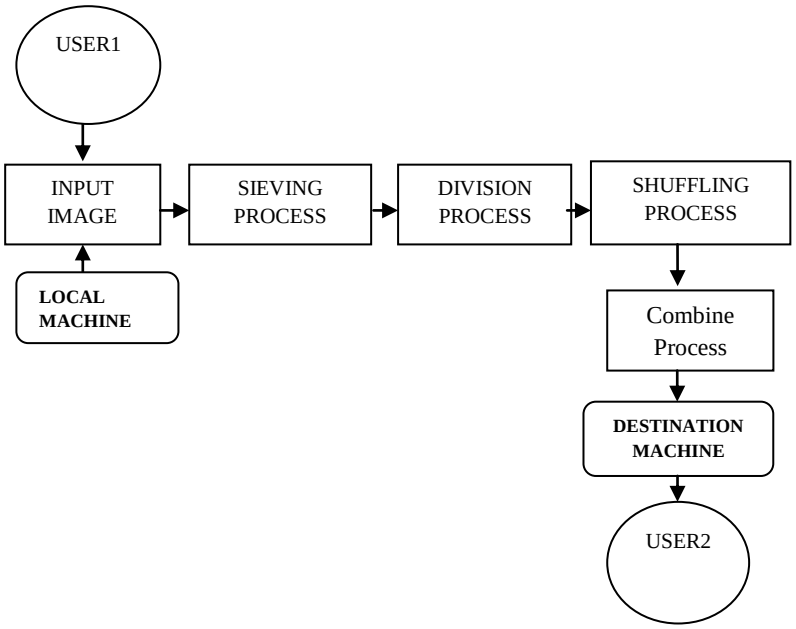

Fig: 2.1 SDS Algorithms

2.1.2 Division

Having filtered the original image into the R, G and B components, the next step involves dividing the R, G and B components into z parts/ shares each.

R _ (RA, RB, RC, ----------, RZ)
G _ (GA, GB, GC, ----------, GZ)
B _ (BA, BB, BC, ----------, BZ)

While dividing it is ensured that each element in RA-Z, GA-Z and BA-Z is assigned values randomly, such that the entire domain is available for randomized selection; in case x = 8, then individual elements should be randomly assigned a value varying from 0- 255. The shares so generated should be such that (RA, RB, RC, ---------- RZ) should regenerate R and similarly for G/B components.

2.1.3 Shuffling

Though experimental results have shown that the random shares created by division in no way exhibit any resemblance to the original image, but as a second step towards randomizing the generated shares i.e. RA-Z, GA-Z and BA-Z, we perform the shuffle operation. This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated.

2.2 Hyper-chaos Based Image Encryption Algorithm

In the paper, Chen zaiping, Li haifen, Dong enzeng, Du yang developed A Hyper-chaos Based Image Encryption Algorithm developed in 2010. Inside this paper present a new image encryption algorithm, within this algorithm, shuffling matrix and diffusing matrix are generate. This is based on Chen's hyper-chaotic system. Firstly, the Chen's hyper-chaotic system is use to shuffle the position of the image pixels, and then use Chen's hyper-chaotic system to confuse the relationship between the original image and the cipher image. Within this paper, a new image encryption algorithm based on hyper-chaos is proposed, it uses an image shuffling matrix to shuffle the pixel positions of the plain-

image and then the states combination of hyper-chaos is used to change the grey values of the shuffled-image. Some security analysis such as key space analysis, key sensitivity analysis, and correlation analysis of two adjacent pixels is given to show that the proposed cryptosystem has a high security level [2].

2.3 Secret sharing technique

A Novel Image Secret Sharing Scheme, Prabir Kr. Naskar, Ayan Chaudhuri, Debarati Basu, Atal Chaudhuri, [3] Secret sharing is a technique for protecting sensitive data, such as cryptographic keys, precisely during transmission over internet. Secret sharing is a technique for protecting sensitive data, such as cryptographic keys, precisely during transmission over internet. Leading to high computational complexity during both sharing and reconstructing phase and most of the popular secret sharing schemes are based on above schemes. Apart from those secret sharing technique, we are suggesting a scheme which deploys simple graphical masking, done by simple ANDing for share generation and reconstruction can be done by simple ORing the qualified set of shares. Not only that, it generates compressed shares that lead to strong protection of the secret image. Nevertheless it confirms confidentiality and integrity as well. This scheme is highly useful where low end processors are used but security is a major challenge [3].

2.4 Image Cryptography

The Genetic Algorithm Approach, Sandeep Bhowmik, Sriyankar Acharyya, to protect our data against unauthorized access, from the time immemorial the first choice has always been to use cryptography [4]. The effectiveness of the protection through encryption depends on the algorithm applied and as well as on the quality of the 'key' used. If a 'key' is badly designed or haphazardly selected, obviously the protection fails to provide proper security and improper access can be gained on the secured information. The first algorithm in cryptographic system design is the algorithm to generate 'key'. It specifies the manner in which the 'key' is to be chosen. This work focuses on a totally new approach towards the 'key' generation for encryption algorithms. Here, Genetic Algorithm (GA), an important method of artificial intelligence has been applied to generate encryption 'key', which plays a vital role in any type of encryption. In our work, a hybridized technique called BlowGA is also proposed which is a combination of Blowfish and GA. Blowfish Algorithm is a conventional method of encryption. Our experimental observations show that the newly-proposed hybridized method BlowGA outperforms both GA and Blowfish Algorithm. [4].

2.5 Secure Keyless Steganography in Lossless RGB Images

A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images, Ankit Chaudhary, J. Vasavada, J.L. Raheja, Sandeep Kumar, Manmohan Sharma, in this approach for hiding text messages in lossless RGB images[6]. The security level is increased by randomly distributing the text message over the entire image instead of clustering within specific image portions. Storage capacity is increased by utilizing all the color channels for storing information and providing the source text message compression. The degradation of the images can be minimized by changing only one least significant bit per color channel for hiding the message, incurring a very little change in the original image. Using steganography alone with simple LSB has a potential problem that the secret message is easily detectable from the histogram analysis method. To improve the security as well as the image embedding capacity indirectly, a compression based scheme is introduced. Various tests have been done to check the storage capacity and message distribution. These testes show the superiority of the proposed approach with respect to other existing approaches. [5].

2.6 Pixel Sieve Method for Visual Cryptography

In the paper [6], An Improved Pixel Sieve Method for Visual Cryptography, Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh, [6] Visual cryptography encodes a secret image into n shares which are distributed to n participants. Pixel Sieve method was proposed recently to encode an image into shares, but the encryption quality is poor. In this paper an improved version of pixel sieve method is proposed to achieve more security then existing pixel sieve method. Based on cross merge and key shifting schemes, the proposed method generates quite noisy and highly secure encrypted images. The simulation shows that the quality of the encrypted images observably better than existing pixel sieve method.

III. PROBLEM DEFINITION

In the, existing system used SDS [4] algorithm, in this algorithm providing number of limitation:

1. To increase the image size.
2. To maintain a key records.
3. Pattern will be easily recognized.
4. Also high computation involved in encryption as also weak security functions issue.
5. Process to easily identify sequences counter.
6. The algorithm has a large enough key space to resist all kinds of brute force attacks.
7. The encryption algorithm is very sensitive to the secret keys.
8. The new encrypted arithmetic not only shuffles the pixel positions of the original-image, but also changes the color values of the original-image.

Image encryptions have applications in internet communication, multimedia systems, medical and military imaging systems. Each type of multimedia data has its own uniqueness such as high correlation among pixels and high redundancy. Thus, different techniques should be used to protect confidential image data from unauthorized access

The motivation behind this research is the growing need for harder-to-break encryption and decryption algorithms as the computer and network technologies to develop. We consider that by proposing SST keyless image encryption and decryption algorithm, it will help to reduce the relationship among image encryption time complexity.

IV. PROJECT OBJECTIVES

To overcome above limitation, to achieve the number of goal, the main objectives of this research will be as follows:

1. To establish a new algorithm for image transformation, and to test and evaluate it.
2. To compute and compare connection vertical and horizontal shuffle different images with and without the proposed algorithm.
3. To compare the security levels of the encrypted images generated by the combination technique and the SST algorithm.
4. To encrypt or decrypt RGB color image will be done.
5. To make image more securable.
6. The operation time of the encryption algorithm is shorter than the SDS algorithm.

V. PREPOSED APPROACH

5.1 SST System

The aim of this research is to improve the security level of the encrypted images using the proposed transformation algorithm. In this proposed technique using a Sieving, shuffling, transformation algorithm for image security .In this research using a (vertical and horizontal shuffling) to shuffle the image pixel bit and then the transformation techniques to covert image into unreadable image format. This algorithm will be used as a pre-encryption transform to confuse the relationship between the original images and the generated ones. Correlation, Shuffling, Transformations have been used to measure the security level of the images. Furthermore, the focus of this research was concerning a bit mapped (bmp) images as well as JPEG (Joint picture expert group) using the SST algorithm.

The proposed technique is implemented with the SST algorithm and involves three steps. Sieving, Shuffling and Transformation .In step one (Sieving) the secret image is split into Primary(R, G, and B) colors [1]. In step two (Shuffling) the shuffled all bit of RGB combination each within itself [4]. In step three (Transformation) using transformed techniques to transform the original file format into unreadable formatted image. Transformation based system have many properties to achieve high security level, such as sensitivity to change initial conditions and parameters, periodicity (a system that tends in probability to a limiting form that is independent of the initial conditions), random behaviour and unstable periodic orbits with long periods. It has very high diffusion and confusion properties that are desirable for cryptosystem.Finally these shuffled pixels reversed get original image.

5.2 Algorithm

Step 1: Start

Step 2: Input: Secret Image

Sieve (Secret Image)

Step 3: Input image and to calculate an image properties width and height. Let S=(R, G, B) where S is sieve image. To get S1: red, S2: green and S3: blue image.

$$S=\begin{pmatrix} R & G & B\ldots.. \\ r_1 & g_1 & b_1\ldots.. \\ \vdots & \vdots & \vdots \\ r_n & g_n & b_n\ldots.. \end{pmatrix}$$

Step 4: To get the red image such as “r” let size of R is m x n [rows, columns] =size =(R) = (m x n)

$$S1=\begin{pmatrix} R\ldots. \\ r_1\ldots. \\ \vdots \\ r_n\ldots. \end{pmatrix}$$

Step 5: To get the red image such as “g” let size of G is m x n [rows, columns] =size = (G) = (m x n) .

$$S2=\begin{pmatrix} G\ldots \\ g_1\ldots. \\ \vdots \\ g_n\ldots \end{pmatrix}$$

Step 6: To get the red image such as "b" let size of B is m x n [rows, columns] =size = (B) = (m x n).

$$S3 = \begin{bmatrix} B \ldots\ldots \\ b_1 \ldots\ldots \\ \vdots \\ b_n \ldots\ldots \end{bmatrix}$$

Step 6: Shuffling Process
n=total number of pixel (0 to n-1)
m=getpixel
width = x
height = y
6.1 vertical shuffling
for i=0 to bm.x-1
select case toggle
(a) case : 0
for j=0 to bm.y-1to get the image pixel position
z= bm.m (i, (bm.y-1)-j)
to set the pixel
then transferred to vertical manner
bmtransfer.setpixel (i, j, z)
next j
Toggle=1
(b) case: 1
for j=0 to bm.y-1
set the pixel and swap to direction of vertical shuffled
bm.m (i, j)
bmtransfer.setpixel (i, j, z)
next j
Toggle=0
next i
6.2 horizontal shuffling
for i=0 to bm.-1
select case toggle
(a) case : 0
To get the image pixel position
for j=0 to bm.x-1
z= bm.m (i, (bm.x-1)-j, i)
to set the pixel
then transferred to horizontal manner
bmtransfer.setpixel (j, i, z)
next j
Toggle=1
(b) case: 1
for j=0 to bm.x-1
set the pixel and swap to direction of horizontal shuffled
bm.m (j, i, z)
bmtransfer.setpixel (j, i, z)
next j
Toggle=0
next i
Step: 7 Transformation Process
T= stores the bmp header information 54byte
7.1 image to base
Convert base 64 byte (image bytes)
7.2 base to image
Convert image byte (base 64 strings)
Output: Encrypted Image.

Step: 8 Stop

5.3 System Architecture

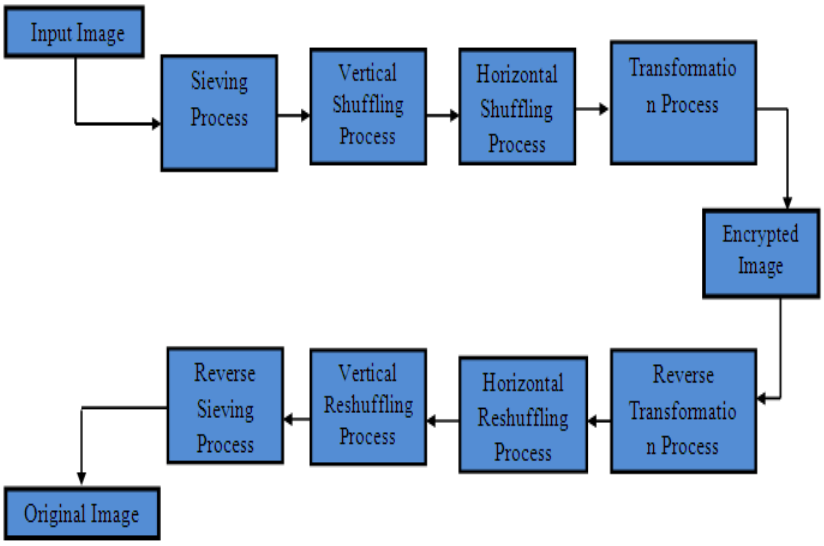

Fig: 5.1System Architecture

In this SST (Sieving, shuffling and transformation) techniques firstly input an original color RGB image. In this image apply the sieving operation to identify the Red, Green and Blue color image in different shades. Then shuffling operation will be done, in this shuffling process apply two shuffled approach: vertical and horizontal shuffling. In this vertical process, shuffled the swap the adjacent pixel bits of image are processed in vertical manner. These images pass into next horizontal shuffling, this process, shuffled the swap adjacent pixel bit of vertical image again processed in horizontal manner and at last this image go to the next stage this transformation process. In this process to identify shuffled image as working BMP image and to BMP file header to use. Inside the Image DES algorithms are through encrypted image and these transformation processes to 54 bit header byte to remove the shuffle horizontal image and then this encrypted image send into the receiver side. In this receiver side just reveres approach to apply. In this reverse transformation process, to add the original file header byte in encrypted image and then pass into horizontal reshuffling process will be done. In this process reshuffled the horizontal adjacent pixel bits arrange and then go next stage, in vertical reshuffling process, to adjacent vertical adjacent pixel bits arrange and reverse sieving process to get different RGB image.

VI. IMPLEMENTATION

6.1 Sieving process

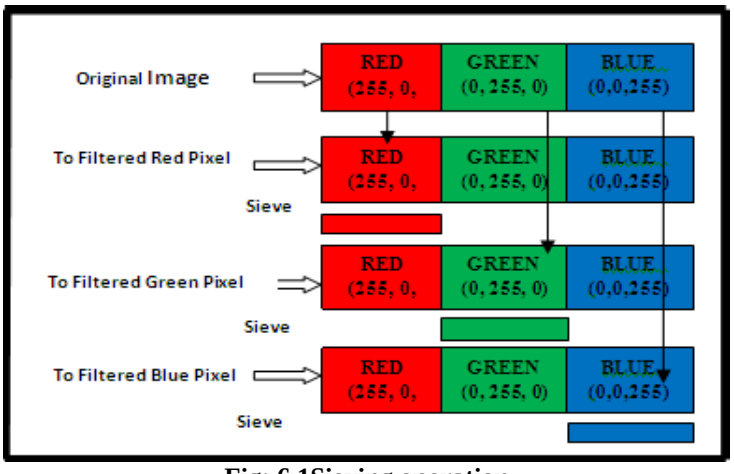

Fig: 6.1Sieving operation

6.2 Shuffling Process

We perform the shuffle operation of sieving image. In these Shuffling techniques also using 2 phases to shuffles the pixel bit in original image. In this module, we are going to using vertical and horizontal pixel bit swap to adjecent pixels value in vertical and horizontal manner.

6.3 Transformation process

In this, transformation process to transform the horizontal image into unreadable image format. This image includes file format header and data .In these images removes the file format header and encrypt the image.

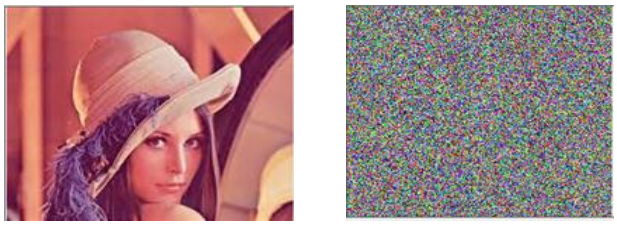

Fig: 6.1 Encrypted Image

VII. EXPERIMENTAL RESULTS

Algorithm	Image Name	Size of Image	No. of Pixels	Features	Proposed scheme
SDS	Leena.bmp	128*128	16384	Noise co-relation	Always increase
				Image delivery Transparency	YES
				Additional Data structure	YES
				Key management	NO
				Pixel Expansions	YES
SST	Leena.bmp	128*128	16384	Noise co-relation	Always 1
				Image delivery Transparency	NO
				Additional Data structure	NO
				Key management	NO
				Pixel Expansions	NO

Fig: 7.1 Comparison between SDS and SST Algorithm

Case	Original Image	Vertical Image	Horizontal Image	Encrypted Image
Image 1 Leena.bmp	 128*128			 128*128
Image 2 Dog.bmp	 275 X 196			 275 X 196
Image 3 Robot.bmp	 374 X 281			 374 X 281

Fig: 7.2 Result Analysis

Embedding Rate(bpp)	0.1	0.2	0.3	0.4	0.5
	PSNR Values According to embedding rate(dB)				
Lena Image 1	54.64	50.35	47.26	44.67	42.58
Dog Image 2	53.59	54.48	45.52	46.25	41.21
Robot Image 3	57.79	51.56	52.56	42.58	40.65

Table: 7.1 PSNR values

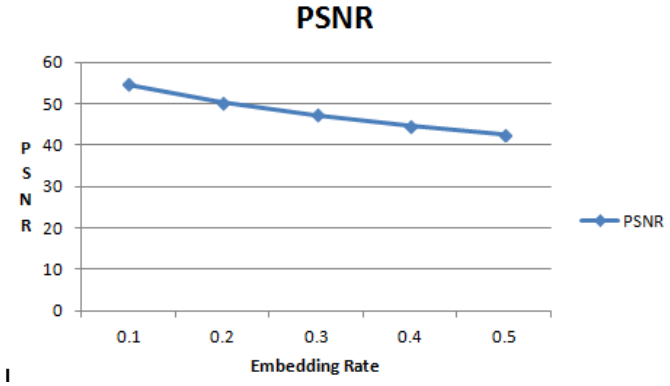

Fig7.3 Lena Image Graph

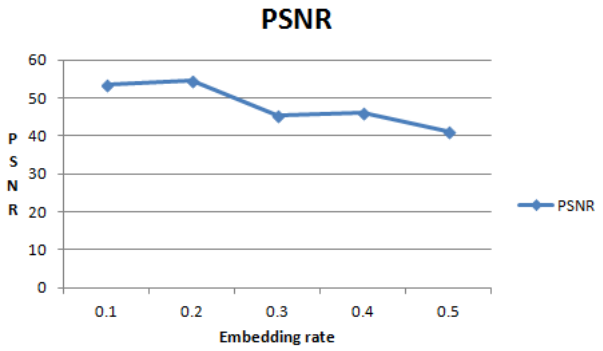

Fig7.4 Dog Image Graph

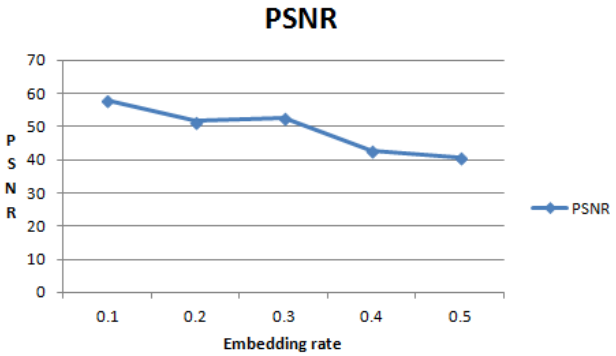

Fig7.5 Robot Image Graph

VIII. CONCLUSION

The procedure of encryption and decryption implemented considered being having better security using SST methods without using any key. In this methods at improving the level of security and secrecy provided by the digital colour image encryption. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image. This new proposed encryption algorithm can ensure the lossless of transmissions of images. The objective of this work is to increase the security level and decrease the CPU computational time. The proposed encryption algorithm in this study has been tested on some images and showed good results.

This paper will describe a new approach to implement keyless approach to lossless image encryption of the every pixel of image and encrypted them. In this proposed work provide the without loss of pixel of any image provided original image quality.

REFERENCES

[1] "A Keyless approach to image encryption" Siddharth Malik, Anjali Sardana, IEEE (2012).
[2] A Hyper-chaos Based Image Encryption Algorithm Chen zaiping, Li haifen, Dong enzeng, Du yang in 2010.
[3] An improved scheme for secret image sharing Saeed Alharthi and Pradeep K. Atrey, 2010 IEEE.
[4] Image Cryptography: The Genetic Algorithm Approach, Sandeep Bhowmik, Sriyankar Acharyya, 2011 IEEE.
[5] "A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images", Ankit Chaudhary, J. Vasavada, J.L. Raheja, Sandeep Kumar, Manmohan Sharma3 The 22nd International Conference on Computer Graphics and Vision and image processing Russia, Moscow, October 01, 2012
[6] An Improved Pixel Sieve Method for Visual Cryptography, Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh, International Journal of Computer Applications (0975 – 8887) Volume 12– No.9, January 2011.
[7] A New Cryptology Approach for Image Encryption, Nidhi Sethi and Deepika Sharma, 2012 2nd IEEE.
[8] A New Encryption Method For Secure Embedding In Image Watermarking, MohammadReza Keyvanpour, Famoosh Merrikh-Bayat, 2010 IEEE.
[9] Image Encryption Algorithm Based on Henon Chaotic System Chen Wei-bin1, Zhang Xin 2009 IEEE.
[10] Keyless user defined optimal security encryption M. Lakshmi, S. Kavitha volume 2 issue 6 2013 International Journal of Engineering and Computer Science.
[11] Analysis on an Image Encryption Algorithm, Shubo Liu1,, Jing Sun, Zhengquan Xu, Jin Liu, 2008 IEEE.
[12] Image Encryption Using Different Techniques: A Review komal D patel, Sonal Belani, International Journal of Emerging Technology and Advanced Engineering, Nov 2011.

