Improvised Steganography Technique using LSB and Rc4 for IOT Applications

Shwetha K R[1] Narayanaswamy G[2]
[1]P.G. Student [2]Associate Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]VVIET Mysuru, India

Abstract— In the present situation, any interaction of online and network application needs protection. Internet protection software is a big issue these days. Lots of data protection and data concealing methods have been developed in the last several years. This is done by using the security and decryption methods. Steganography and cryptography are the two major methods of secret interaction. The program uses an RC4 stream cipher technique to turn plain text into cipher text criteria which has very good efficiency and is a most highly effective strategy compared to other Algorithms, then use least significant Bit (LSB) technique to include the secret written text in an image and then it will be used the specific location. Where it is decrypted and unique concept is acquired and provided. Our suggested model gives two levels of to protect secure information, which fully fulfill the basic key factors of information protection program that includes: Privacy, Authenticity, Reliability and Non – Repudiation. In this paper I have applied FPGA based steganography strategy.

Key words: Steganography, LSB technique, Cryptography, RC4 stream cipher, FPGA

I. INTRODUCTION

Since the growth of the internet, the first thing of technological innovation and interaction has been the security of data. Many different methods have been designed to secure and decrypt information in order to keep the concept secret. Sometimes it is not enough to keep the material of a concept key, it may also be necessary to keep the use of the concept key. Steganography is the process used for this. Steganography is the technological innovation and art of unseen interaction of information. This is done by concealing details in an image, ie. Hiding the use of the conveyed details. The phrase steganography comes from the Ancient terms "stegos" significance "cover" and "grafia" significance "writing" interpreting it as "covered writing". Steganography is mostly used on computer systems with digital information being the providers and systems being the high-speed distribution programs. Cryptography is a technological innovation of key composing. It is the art of defending the details by changing it into an un-readable structure in which a concept can be disguised from the informal audience and only the designed receiver will be able to turn it into the very first written text Steganography and cryptography, both are ways for defending details from unwanted parties. These technological innovations are mainly concerned with the protection of intellectual property. This paper explains the LSB criteria used for image steganography for example the protection potential of steganography for business and personal use. The difference between Steganography and Cryptography is that the cryptography concentrates on keeping the contents of a message secret whereas steganography concentrates on keeping the existence of a message secret. Many criteria are used in cryptography.RC4 stream cipher technique used for multilayer to protect information. RC4 turn simply written text into cipher written text, then included the information by using LSB technique. The suggested technique should provide better protection while shifting the information or information from one end to the other end. Primary of the work is to cover up the concept or key information into a picture which functions as a service provider file having key information and to deliver to the location safely without any adjustment. If any disturbances occur in the picture or on its quality, while placing the key concept into the picture, there may be a chance for an illegal person to change the information.

II. LITERATURE REVIEW

Armin Bahramshahry et al.[3] in 2007 provided a technique based on picture position. First of all, key information is secured using RSA security criteria and then users choose any picture suitable for concealing particular information. This will make difficult for the enemy to be successful an attack. Lastly, a stego picture has been produced, but this paper does not have in reliability and this application cannot cover up large data.

S. Channalli, A. Jadhav et al.[4] in 2007 writers determine a technique of concealing information on the billboard. This approach can be used for introducing a key concept in public place. User first goes into the regular information then conceals key information into regular information and the secured information is shown on the billboard board. This secured information is stored for decrypting the key information.

Chunlin Music et al. [5] during 2009 have provided information and research into the recent developments in the watermarking in digital pictures. These techniques are sorted into the several groups based on the sector in which invisible information is placed, size of invisible information, and the need of which invisible information is to become. The research shows the different effective methods of watermark. The result indicates regularity sector is more sturdiness than spatial sector. Several difficulties that are often unaddressed in the literary works have also been recognized.

Shamim Ahmed Laskar et al. [6]The present technique an attempt to recognize the specifications of a reliable information concealing criteria. Steganography is not the answer to secrecy, but neither is security. But if these methods are mixed, we will have two levels of protection. If an email is secured and invisible with a LSB steganographic technique the embedding potential enhances and thus we can cover up large number of information. And the process meets the specifications such as potential, protection and

sturdiness which are meant for information concealing. The suggested criteria is examined in the light of the mathematical structure in order to confirm its efficiency and also to show its degree of protection.

Shilpa Gupta et al.[7] this year, In this document current Least Important Bit Algorithm has been examined and found to have a more amount of distortions, so a new technique has been suggested "Enhanced Least Important Bit (ELSB). It enhances the efficiency of the LSB technique because information is in visible in only one of the three shades that is BLUE colour of the service provider picture. This reduces the distortions stage which is irresponsible to human eye.

Shilpa Thakar et al.[8] in 2013, this document explain the overview of Steganography. Picture Steganography along with the LSB placement method used in Picture Steganography. The document recommended a few for upcoming research like reliability and information potential of protecting the image. Some steganographic techniques need to increase protection by using cryptography against strikes.

G. Raj Kumar et al. [9] in 2014, have been enhanced least important bit steganalysis by examining and adjusting popular functions of the some current least important bit related steganalysis techniques. This document describes the LSB Embedding strategy with raising based DWT techniques by using Small fire Processer applied in a FPGA using System C programming. Future work can be prolonged to RGB or shade image handling and can be prolonged for video handling level also.

III. CONCEPT OF STEGANOGRAPHY

Steganography is the method of embedding hidden messages in such a way that no one, except the emailer and designed receiver(s) can identify the existence of the information. The primary purpose of steganography is to protect the key idea or information in such a way that eavesdroppers are not able to identify it. If they found any dubious information, then the objective is beaten. Other purpose of steganography is to connect safely in a completely invisible way. The many types of information in steganography can be audio, video, text and pictures etc. fig1 reveals idea of steganography. The primary kind of Steganography comprises of three elements:

The Carrier image: The carrier picture is generally known as the cover item that will bring the message that is to be hidden.

- The Message: A message can be anything like information, data file or picture etc.
- The Key:A key is used to decode/decipher/discover the invisible idea.

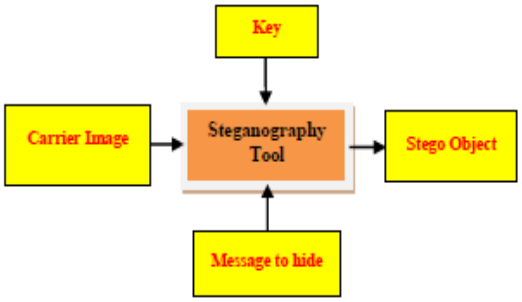

Fig. 1: Concept of steganography

A. Types of Steganography

The various types of steganography include

1) Image Steganography

The image steganography is the procedure in which we cover up the information within a picture so that there will not be any perceivable modify in the original picture. The traditional image steganography criteria are LSB embedding algorithm.

2) Audio Steganography

The method of concealing secret information in a audio is known as audio steganography. There are various techniques for concealing key information in a sound such as LSB, Stage Programming etc.

3) Video Steganography

The method of hiding secret information in the videos is known as video steganography. Video involve pictures as well as audio. Hence, both image and audio steganography can be used for video steganography.

4) Text Files Steganography

The method of concealing key information in a text is known as written text steganography. Text steganography needs less storage as it can only shop written text information files. It provides quick interaction or exchange of information files from one computer to another.

B. Cryptography

Cryptography is the art of accomplishing security by developing information to make them non-readable. Cryptography is an art of transferring the information securely over the Internet by making use of some cryptographic methods so that it will be difficult for an opponent to strike or grab some private or personal information. Two basic terms used in cryptography is encryption and decryption; security is the operation of transforming simply written text into cipher written text and decryption is the reverse procedure of encryption . Plain written text is the writing having the actual concept or information which is not secured and cipher written text is the writing after security of concept or information which is ready to be distributed.fig 2 shows prevent plan of cryptography.

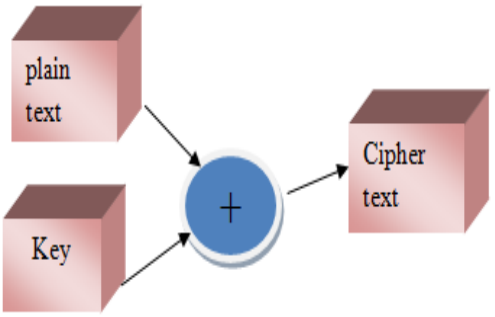

Fig. 2: Block diagram of Cryptography

C. Least Significant Bit Insertion

The technique converts image into a shaded Gray Range picture. This area will be becoming the referral picture to cover the written text. Using this gray scale referrals image any written text can be invisible. The Single personality of a written text can be showed by 8-bit. If the referral picture and the computer information file are passed on through network independently, we can achieve the effect of Steganography. Here the picture is not at all altered because

said picture is only used for referencing. Any large amount of written text material can be invisible using a very small picture. Figure out the written text is not possible intercepting the picture or computer information file independently. So, it is more secure. In this method the least significant components of some or all of the bytes of a picture are substituted for a component of the secret concept.

D. Pixel Processing

After the transforming our details secret rule or secured type we need to spot that detail in the picture. We use least important bit for the patching of data because of following purpose.

a) Because the strength of picture modifies by 1 or 0 after concealing the details.
b) The Alternation in strength is either 0 or 1 because they modify at last bit .e.g. 11111000 11111001

The modify is only one bit so that the strength of the picture is not impacted too much and we can readily exchange the details.

Steps To Place Data In Image:-

a) Take a port picture.
b) Find out the pixel principles.
c) Select the pixel on which we want to insert data

This procedure of collection of pixel is done as user's option he may choose pixel ongoing or different or at a limited range. Place the details principles in p eg. For example a line for 3 p of a 24-bit picture can be as follows:

00101101 00011100 11011100
10100110 11000100 00001100
11010010 10101101 01100011

When the number 200, which binary reflection is 11001000, is included into the least important pieces of this part of the picture, the causing lines is as follows

00101101 00011101 11011100
10100110 11000101 00001101
11010010 10101100 01100011

E. Rivest Cipher-4 Method

There are so many stream ciphers in these days, these stream ciphers are really easy to apply in components, but may not be in the application. Later, Ron Rivest designed the RC4 flow cipher. It is correct for software, and is used commonly these days. For example, RC4 is used in SSL (Secure Electrical sockets Layer) method. It is also be used in WEP (Wired Comparative Privacy) and many system programs.RC4 is the most commonly used flow cipher in these days, unique for the programs. This is because the framework of RC4 really is easy and can be applying in software effectively. Although RC4 has a large inner condition, it has the light-weight key arranging and the outcome creation procedures. Fig 3 shows block diagram of RC4

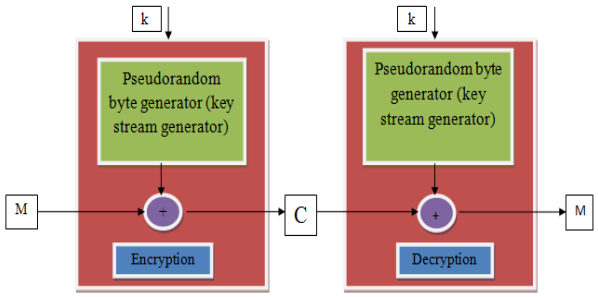

Fig. 3: Block diagram of RC4

IV. PROPOSED SYSTEMS

To improve the embedding potential of picture steganography and provide an imperceptible stego picture for human perspective, we recommend a structure for concealing large amounts of information in pictures by mixing cryptography and steganography while running into little perceptual deterioration and to resolve the problem of illegal information access. Steganography also can be applied to cryptographic information so that it improves the protection of this information. In this technique we first encrypt message using RC4 cipher technique and then embed the encrypted message inside an image using LSB embedding technique. The mixture of these two methods will improve the protection of the information included. This combinational technique will fulfill the specifications such as capacity, security and robustness for secure information transmitting over an open route. The causing stego-image can be passed on without exposing that secret information is being interchanged. Furthermore, even if an opponent were to beat the steganographic technique to identify the concept from the stego-object, he would still require the cryptographic understanding strategy to figure out the secured concept. Fig 4 shows RTL Prevents for FPGA Implementation

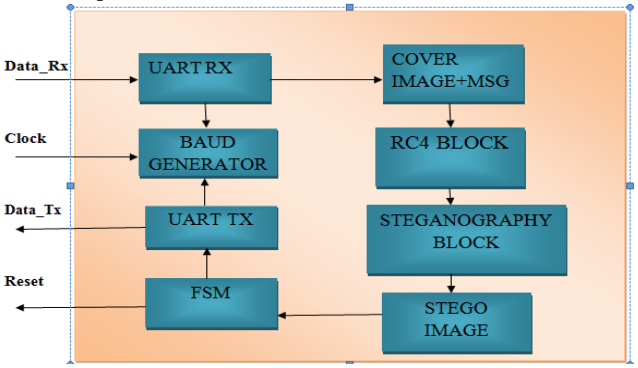

Fig. 4: RTL Blocks for FPGA Implementation

The suggested program appears for two primary levels these are:-

1) Embedding key written text in the still picture by using one (LSB Technique) from many suggested methods of steganography concealing.
2) Getting the stego written text from many stego-objects (image) when picture obtained to other part.

A. Embedding Stage

Embedding is the process of concealing the embedded message producing the stego picture. Hiding details may require a Stego key which is additional key details, such as security password, required for embedding the details .For

example, when a key concept is invisible within a protect picture, the causing product is stego picture (stego object).
The main criteria for the Embedded level can be detailed as follows:-

1) Feedback the secret written text (message) that to be invisible in the cover image.
2) Choose the cover image (BMP file) from a list of picture with dimension 64*64.
3) Open the cover image and read the information in the matrix
4) Determine the dimensions of the secret text
5) Apply RC4 stream cipher on secret text
6) Alternative Substitute the encrypted secret characters of the text in the specified location (hope value) of the cover image

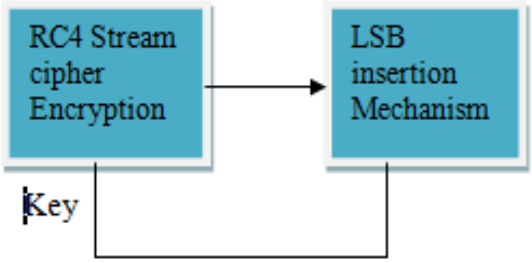

Fig. 5: Block diagram for encoder

The block diagram of the encoder is shown in the fig 5. The encoder involve two levels ,the first level is the RC4 flow cipher which secure each byte of the key written text before to the embedding procedure, the preliminary key of this function is a unique permutation. The second level of the encoder is the LSB placement procedure, randomization of placement the key concept pieces into the picture is confirmed by the utilizing of the balanced out ,by this procedure include each bit from the ciphered secret written text into 8-pixels from the protect picture

B. Extracting Stage

Extracting is the procedure of getting the included message out of the stego item again. After the stego object then is designed and passed on through a interaction route, if we believe perfect route the stego item is obtained effectively by the decoder routine, again the decoder has two information (the removal key and the stego object) and individual outcome which is the key written text. The succession of function here is changed, the LSB from stego item is first done then the ciphered key written text byte is obtained, after that the last level of RC4 decryption is done, the prevent plan of this function is shown in the fig 6.

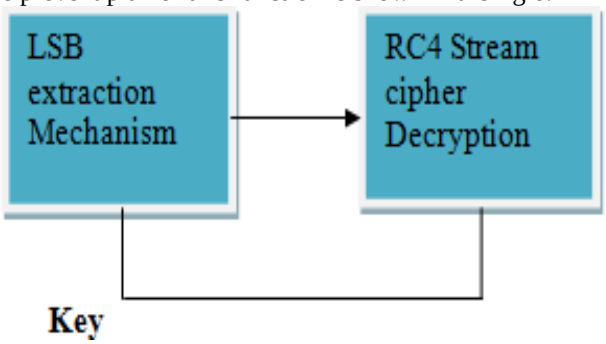

Fig. 6: Block diagram for decoder

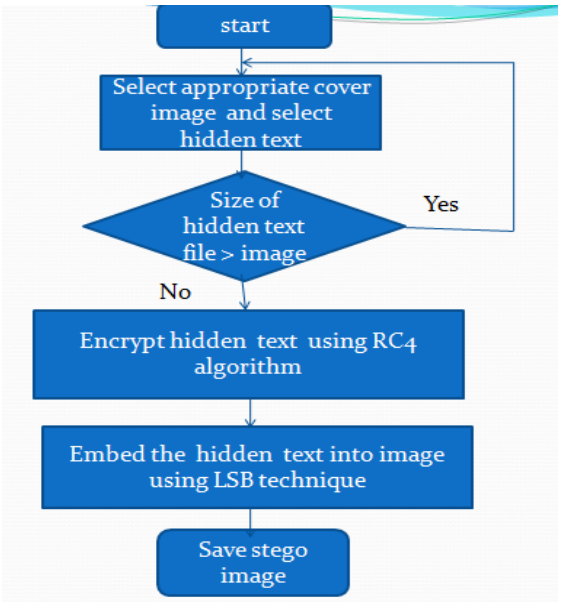

Fig. 7: Flow chart of overall operations

V. EXPERIMENTAL RESULTS

This style is achieved via Verilog HDL components information terminology by Xilinx 13.2 application simulated with MATLAB, and lastly applied on FPGA in Spartan-3A members of the family. Power is examined to Xilinx power. This design has a high-speed, great throughput and low power intake. It is really appropriate for extremely properly secured picture security and also the time of its transforming is low. Fig 8 shows Simulation result. Fig 9: Original Image and Encrypted Image

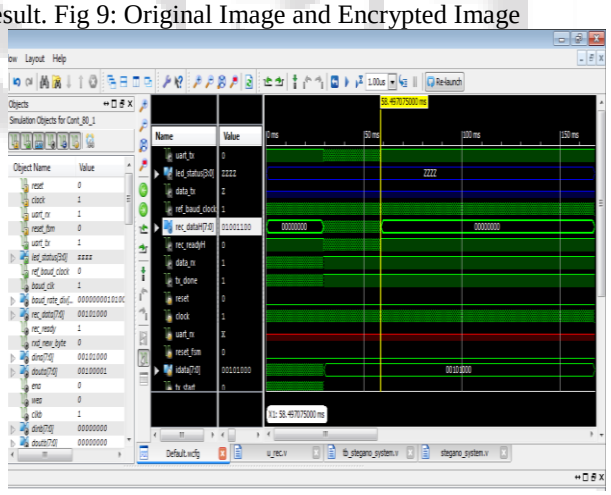

Fig. 8: Simulation result

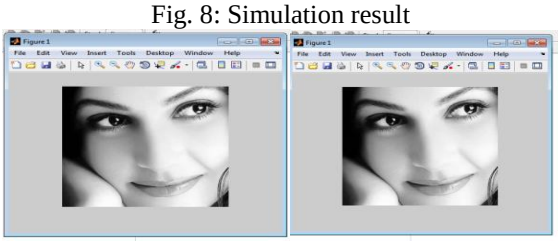

Fig. 9: Original Image and Encrypted Image

Device Utilization Summary(estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	152	5888	2%
Number of Slice Flip Flops	142	11776	1%
Number of 4 input LUTs	283	11776	2%

Number of IOs	10		
Number of bonded IOBs	6	372	1%
Number of BRAMs	9	20	45%
Number of GCLKs	2	24	8%

Table 1: Device Utilization Summary

Timing Summary	
Factors	Values
Speed Grade	-5
Minimum Period	2.384ns
Baud Rate	9600bits/sec
Maximum Frequency	170.35MHz
Minimum input required time after clock	5.270ns
Maximum output required time after clock	6.839ns

Table 2: Timing Summary

FPGA Device	XC400E-4013EPQ208-2	XC2V250fg256	XC3S700fga484-5
Number of Slice Flops	255	135/3072	152/5888
Frequency (MHz)	40	164.6	173.35

Table 3: Hardware Resources and Frequency Comparison

Table 1 shows Device Utilization Summary, Table 2 shows Timing Summary, Table 3 shows Hardware Resources and Frequency Comparison.

VI. Security of Proposed System

With regards to Steganography is to prevent illustrating suspicion to the transmitting of invisible details, if suspicion is brought up, then Steganography protection is defected. On the other hand the aim of cryptography is to change intelligible details to unintelligible form, hard the third events which not have a duplicate from the key. The suggested program accomplishes the partnership objective of protection for the below reasons:

1) The results of suggested program stego-object is an picture, this picture is passed on alone without the very original picture, this point increases the protection of program because there is little capability of related between the very first protect picture and the stego-object.
2) The suggested program is designed on multilayer protection, consequently even if the very original duplicate of the stego-object is available, the burglar assaulted by the second part of protection which is the security of the writing included then he should evaluate the cipher written text using cipher written text only strike which is hard to be examined.
3) The security password level of protection is also included to our program, this part of protection should not be combined with the two above levels, because it program focused security layer , not security gained by algorithm presented ,but it still effective and add more rigidity to the proposed system.

VII. Conclusion & Future Scope

The suggested programs provide LSB technique with RC4 stream cipher and expect embedding written text in image. A number of results were produced from this study

1) Steganography is not designed to replace cryptography but rather to complement it. If a message is secured and invisible with a steganographic technique it provides an additional part of security and decreases the chance of the invisible message being recognized.
2) The proposed system can be defined as secret key steganography since it stocks a secret key between emailer and recipient, in this program there is no need for the knowledge of unique protect in the removal procedure.
3) The quantity of the information a part of the other media relies upon on the mathematical qualities of the protect media, where this quantity is small the disturbance on media is not obvious.
4) From the execution we determine that the suggested program is very fast in executing removal procedure and the size of the included written text does not impacted the rate of the program very much

Many recommendations can be given to improve the work of the proposed program they are:-

1) The process of embedding is simple which is LSB insertion, in the upcoming another embedding technique should be employed like wavelet or DCT convert centered techniques.
2) Enhanced program to handles movie picture and sound.
3) Using another data structure of pictures that are not used in our program such as JPEG, TIFF and GIF.
4) The Protection technique (RC4) could get changed with RSA, or other community key ciphering criteria to improve the security level.

References

[1] Katzenbisser, S, and Fabien A.P. Petitcolas," Information Hiding Techniques for Steganography and Digital Watermarking" Artech House, Bosten, London, 2000.
[2] Dorothy E. and R. Denning, "Cryptography and Data Security", Addison – Wesley publishing company, Inc., 1983.
[3] Armin Bahramshahry, Hesam Ghasemi, Anish Mitra, Vinayak Morada,Design of a Data Hiding Application Using Steganography", Databases, 2007, pp. 1-6.
[4] S. Channalli, A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol.1 (3), 2009, pp. 137-141.
[5] Chunlin Song, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images", ISBN: 978-1-902560-22-9,2009PGNet.
[6] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems, Vol.4, No.6, December 2012.
[7] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, " Enhanced Least Significant Bit algorithm For Image Steganography", International Journal of Computational Engineering & Management, ISSN (Online): 2230-7893, Vol. 15 Issue 4, July 2012.
[8] Shilpa Thakar, "Review of Image Steganography", International Journal of Computational Engineering &

Management, ISSN (Online): 2230-7893, Vol. 15 Issue 4, July 2013.

[9] G. Raj Kumar, M. Maruthi Prasada Reddy and T. Lalith Kumar, "An Implementation of LSB Steganography Using DWT Technique", International Journal of Engineering Research and General Science, ISSN 2091-2730, Volume 2, Issue 6, October-November, 2014.

[10] Pooja Kaushik and Yuvraj Sharma, "Comparison of Different Image Enhancement Techniques Based Upon Psnr & Mse", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11, 2012.

