ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

STEGANOGRAPHY USING RC4 ALGORITHM

Prayag s. Desale*, Gajanan m. Burande, Gaurav s. Aggarwal, Mr. P.m.ghate

* Department of Electronics and Telecommunication Engineering JSPM's Rajarshi Shahu College of Engineering Savitribai Phule Pune University, Maharashtra, India

Department of Electronics and Telecommunication Engineering JSPM's Rajarshi Shahu College of Engineering Savitribai Phule Pune University, Maharashtra, India

Department of Electronics and Telecommunication Engineering JSPM's Rajarshi Shahu College of Engineering Savitribai Phule Pune University, Maharashtra, India

Department of Electronics and Telecommunication Engineering JSPM's Rajarshi Shahu College of Engineering Savitribai Phule Pune University, Maharashtra, India

ABSTRACT

Steganography is art of hiding data using a image is discussed in this paper.This is done by using the encryption and decryption techniques.Internet security is a big issue nowadays. Specially the areas where highly confidential and secret data is needed to be transferred, there is a possibility that confidential data might be hacked. So, it is necessary to provide a high level of security to the secret data. Hence we have built a device which can capture an image in real time and send it over internet. We have built a device that can be used to transfer secret data over internet.Using this device encrypted data will be hidden inside an image with help of the rc4 algorithm and then it will be transferred to respective destination.Where it is decrypted and original message is obtained and delivered

KEYWORDS: Encryption,Decryption,Steganography,RC4

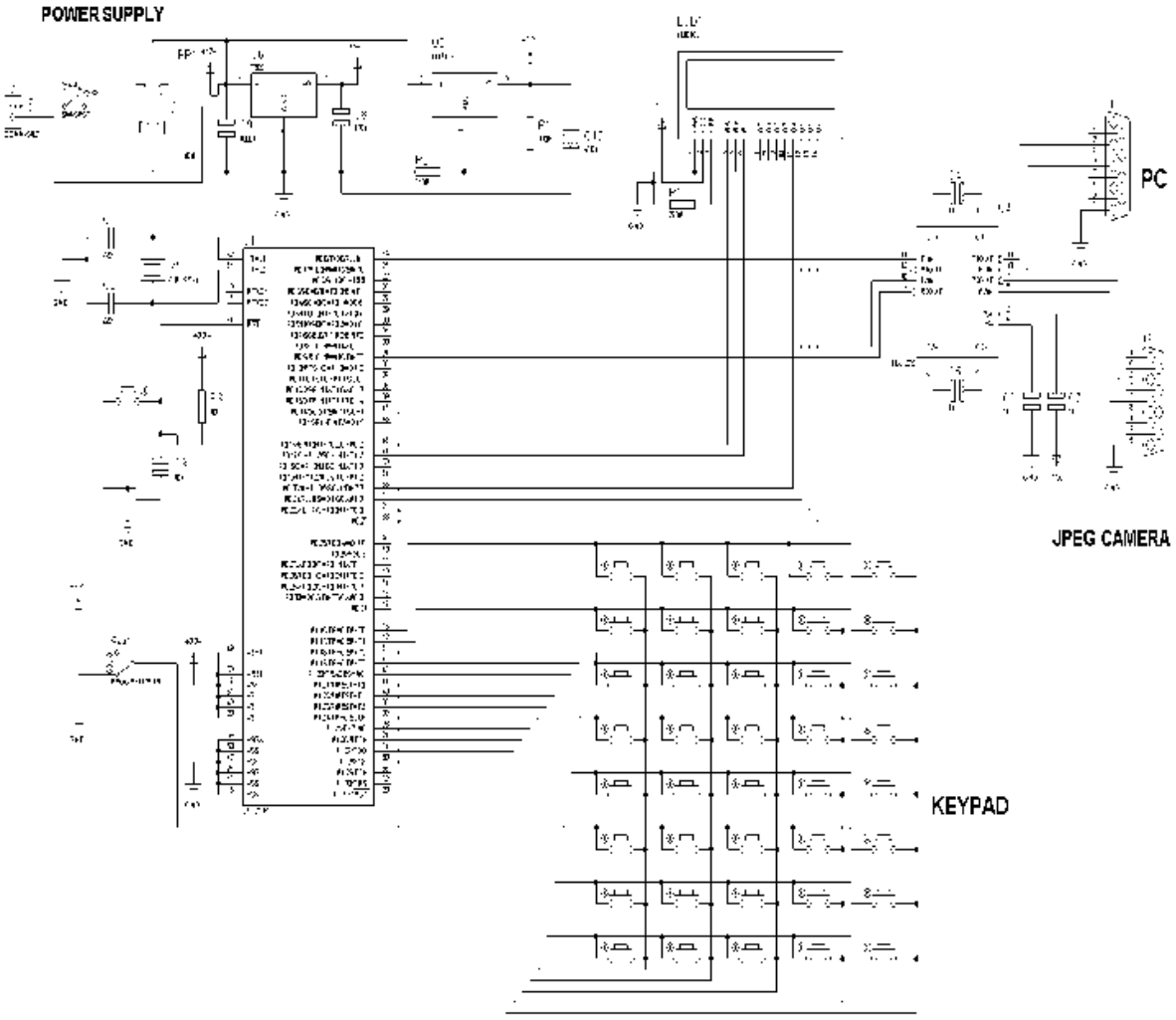
INTRODUCTION

With the ever increasing amount and variety of data to be stored and transmitted in various mediums, the specification of security which has to be established at various levels of medium access and the accompanying issues of authentication and authorization has become a critical factor. Various steganographic, watermarking and data-embedding algorithms have usually manipulated the actual data in order to either hide any coveted information or to provide some level of access control over the medium. The mediums are usually images, video, audio etc., wherein specific portions or the overall space is usually 'corrupted' with 'significant' data. We attempt to bring out the significance of the steganographic techniques that are employed in information processing algorithms for data security. It deals with the problem of data security, focusing mainly on images, and tries to state the various properties and characteristics that the steganographic algorithms should possess. We also highlight the technique of masking used in the conventional steganographic LSB algorithms and in its variants.

It helps in understanding different image formats.(jpeg, bmp). It requires learning of steganography, cryptography algorithms. Implementation of steganographic algorithm in ARM processor. Studying interfacing of camera and interfacing of keyboard with ARM.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

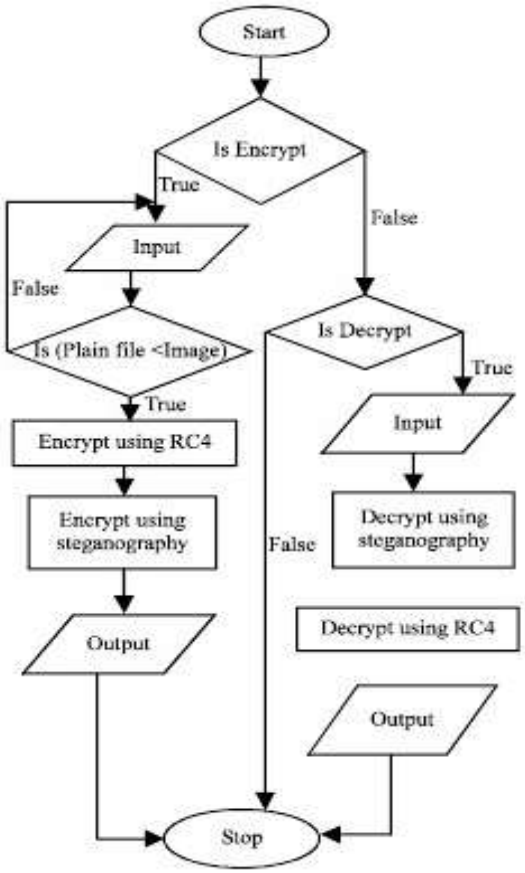
WORKING PRINCIPLE



A power supply according is designed to supply enough power to run the ARM7(LPC2148)and the camera.µCAM camera module is interfaced with ARM7 (LPC2148).Matrix keyboard (8*5) qwerty type of keypad to enter data to be encrypted is interfaced to ARM7(LPC2148). Highly confidential data entered with keyboard is hidden inside an image.Before transmitting the image to specified user , we will encrypt data by using RC4 algorithm. Then on this encrypted data , we will apply data encryption standards.There is user interface designed using VB(Visual Basic) language where we can visualize our image taken by camera. This image is being saved on our local pc. Recipent is having one VB interface application on his own pc where and decryption algorithms are applied. Thus that confidential data is accessed by the intended recipient. Here the ARM7 plays and important role in encryption and decryption process were the image is accesed by the ARM7.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

FLOW CHART



RC4 ALGORITHM

The RC4 algorithm generates a pseudo-random key stream that is then used to generate the ciphertext (by XORing it with the plaintext). It is called pseudo-random because it generates a sequence of numbers that only approximates the properties of random numbers. The sequence of bytes generated is not random since the output is always the same for a given input but it has to approximate random properties to make it harder to crack. The key stream is generated from a variable length key using an internal state composed of the following elements:

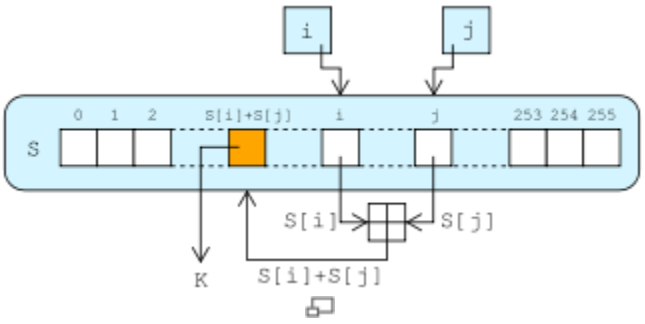
A 256 bytes array (denoted S) containing a permutation of these 256 bytes Two indexes i and j, used to point elements in the S array (only 8 bits are necessary for each index since the array only have 256 elements)

Once the S array has been initialized and "shu_ed" with the key-scheduling algorithm (KSA), it is used and modi_ed in the pseudo-random generation al-gorithm (PRGA) to generate the keystream.

```
for i from 0 to 255
   S[i] := i
endfor
j := 0
for i from 0 to 255
   j := (j + S[i] + key[i mod keylength]) mod 256
   swap values of S[i] and S[j]
endfor
```

The pseudo-random generation algorithm (PRGA)

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

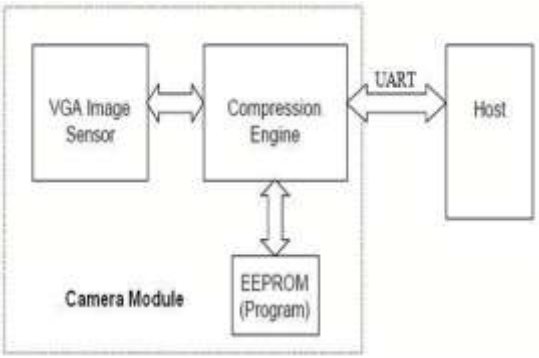


The lookup stage of RC4. The output byte is selected by looking up the values of S(i) and S(j), adding them together modulo 256, and then looking up the sum in S; S(S(i) + S(j)) is used as a byte of the key stream, K.

For as many iterations as are needed, the PRGA modifies the state and outputs a byte of the keystream. In each iteration, the PRGA increments *i*, looks up the *i*th element of S, S[*i*], and adds that to *j*, exchanges the values of S[*i*] and S[*j*], and then uses the sum S[*i*] + S[*j*] (modulo 256) as an index to fetch a third element of S, (the keystream value K below) which is XORed with the next byte of the message to produce the next byte of either ciphertext or plaintext. Each element of S is swapped with another element at least once every 256 iterations.

```
i := 0
j := 0
while GeneratingOutput:
   i := (i + 1) mod 256
   j := (j + S[i]) mod 256
   swap values of S[i] and S[j]
   K := S[(S[i] + S[j]) mod 256]
   output K
endwhile
```

JPEG CAMERA



There are other Start Of Frame markers that introduce other kinds of JPEG encodings.Since several vendors might use the same APPn marker type, application-specific markers often begin with a standard or vendor name (e.g., "Exif" or "Adobe") or some other identifying string.At a restart marker, block-to-block predictor variables are reset, and the bitstream is synchronized to a byte boundary. Restart markers provide means for recovery after bitstream error, such

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

as transmission over an unreliable network or file corruption. Since the runs of macroblocks between restart markers may be independently decoded, these runs may be decoded in parallel.

EQUATIONS

Here we are using core type transformer with N2:N1 is 12:1. FORMULA FOR TRANSFORMER:N2/N1 = I2/I1 = V1/V2 As we know input voltages from Mains to transformer are not constant it's varying from 220V to 270V. If we took 15V transformer so the input voltage of transformer is Standard value i.e 230V, but if the Input voltages are varying the required voltages are also varying. Therefore we assume the highest possible value of Input voltage is 270V so the output voltage is 19V.

The average voltage at the output of a bridge rectifier capacitor filter combination is given by

$$Vin(DC) = Vm - Idc / 4 f C1$$

Where ,$Vm=\sqrt{2}\ Vs$ and Vs = rms secondary voltage
Assuming Idc to be equal to max.load current, say 100mA

$$C = 1000\ Gf / 65v\ ,\ f=50hHz$$
$$19 = Vm - 0.1 / 4*50*1000*10^(-6)$$
$$19= Vm - 0.1 / 0.2$$
$$Vm=19.5\ volts$$

Hence the RMS secondary Voltage

$$Vrms = vm/ \sqrt{2}$$
$$= 19.5 / \sqrt{2}$$
$$=19.5 / 1.4421$$
$$=13.5219\ volts$$

So we can select a 15v secondary Voltage
Min Input for 7812 is
So at Input of 7812 we required 15 V supply.
Consider drop across diode 0.7V so 2 diode conducts drop is 1.4 V

$$= 15\ V - 3\ V$$
$$= 12\ V$$

So at secondary we required 15 V
E0 min/E0 max = (15-0.7) / 15+0.7

$$= 14.3 / 15.7$$
$$\theta 1 = \sin^{-1} [0.9108]$$
$$= 65.616°$$

After LM7805 we got exact 12V.
Min Input for 7805 is = Drop across IC 7805 + Required Output voltage

$$= 3\ V + 5V = 8\ V$$

So at Input of 7805 we required 8 V with margin
Consider drop across diode 0.7V so 2 diode conducts drop is 1.4 V

$$= 1.4\ V + 8\ V$$
$$= 9.4\ V$$

So at secondary we required 10 V

$$E0\ min/E0\ max = (10-0.7) / 10+0.7$$
$$= 9.3 / 10.7$$
$$\theta 1 = \sin^{-1} [9.3/10.7]$$
$$= 60°$$

RECTIFIER
For bridge

$$T1 = [time\ for\ 90° + time\ for\ \theta 1]$$
$$= 5ms + 3.4ms$$
$$= 8.4ms$$

Il = load current supplied to various IC

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

Il = (O/P current of IC PIC16F877A or ARM-7 + O/P current of IC 232 + Current req. for display)
= 71mA + 30mA + 15.2 mA = 116.2 mA

C = (Il * t1)/Vr
= (116.2 mA * 8.4 ms)/ 1 V
= 976.04 µf

So we select 1000 µf capacitor

For diode design

PIV = Vm

Vm = E0 max + 2 Vf
= 10.7 + 1.4 V
= 12.1 V

I(0) = I(1) /2
= 116.2 mA/ 2
= 58.1 mA

Peak repetitive current

Ifm = [I(1) (t1+t2)]/t2

T2 = time for 90° - time for θ1
= 5ms - 3.4ms
=1.2ms

Ifm = 116.2 mA(8.6ms+1.2ms) /1.2ms.
=833mA

From above specification diode 1N4007 is selected

PIV =100V

I = 1A

a)The TUF is increased to 0.812 as compared the full wave rectifier.

b) The PIV across each diode is the peak voltage across the load =Vm, not 2Vm as in the two diode rectifier

Output of the bridge rectifier is not pure DC and contains some AC some AC ripples in it. To remove these ripples we have used capacitive filter, which smoothens the rippled output that we apply to 7805 regulators IC that gives 5V DC. We preferred to choose capacitor filters since it is cost effective, readily available and not too bulky.

The value of the capacitor filter can be found by following formula,

C = IL * t1

C1 (1000 µf / 65v) is the filter capacitor and C2 and C3 (0.1 uf) is to be connected across the regulator to improve the transient response of the regulator.

A regulator is a circuit that supplies a constant voltage regardless of changes in load current. The regulator used in our project is IC7805, which is a three terminal voltage regulator. A heat sink is used, so that the heat produced by the regulator dissipating power has a larger area from which to radiate the heat into the air by holding the case temperature to a much lower value than would result without the heat sink.

IC 7805 has an internal thermal overload protection and the internal short circuit current limiting device.

The AC mains are given to the transformer primary to get the required voltage at the secondary. Then it is applied to the bridge rectifier, which converts the sinusoidal input into full wave rectified output. The output of the rectifier contains some ripple voltage. To remove this voltage filter circuit is used. A ripple voltage is nothing but a small value of AC over DC signal. Then a pure DC is given to the regulator. The function of the regulator is to give the constant or stable output DC in spite of changes in the load current.

The reasons for choosing IC regulator is that they are versatile in operation and relatively inexpensive with features like programmable output, current/voltage boosting, internal short circuit current limiting, thermal shutdown.

The 78XX are popularly known for regulation has been used. The 78XX series is a 3-terminal positive voltage regulator and 79XX series is a 3-terminal negative voltage regulator.As name suggests it transforms the voltage level from one level to another. Transformer used is the step down transformer to step 230 V to +15 V.
It provides isolation too from the mains.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

Now we design 3.3V for Microcontroller ARM-7

The formula for calculating the output voltage of ARM is (As given in the datasheet of LM1117)

Formula:-

1.5V = Vin- Vout

Here we know Vin=5V.

So, 1.5V = 5V - Vout

Vout = 5V - 1.5V

= 3.5V.

Therefore we get an o/p of 3.5V, so we are taking from here 3.3V.

ACKNOWLEDGMENT

We express our deepest sense of gratitude towards our Honorable Head of department Prof G. C. Patil for giving permission to use the college resources and his constant encouragement for this work.

We are grateful to Mr. P. M. GHATE for his technical support, valuable guidance, encouragement and consistent help without which it would have been difficult for us to complete this project work. We are thankful to our entire staff of Electronics and Telecommunication Department for their timely help and guidance at various stages of the progress of the project work.

REFERENCES

[1] Al-Ataby ,A and F. Al-Naima ,2010 A modified high capacity image steganography ,technique based on wavelet transform.int Arab J Inform .technol.:358-364

[2] Curran.k and k.bailey 2003 an evaluation of image based steganography methods.Int.J.Digital Evid..2:1-40

[3] Cheddad.A.J.Condell,K.Curran and P.Mckevitt,2010.Digital steganography:Survey and analysis of current methods.Signal Process,90:727-752

[4] Pardeep and P.K.Pateriya,2012.PC1-RC4 and PC2-RC4 algorithms:pragmatic enrichment algorithms to enhance RC$streamcipheralgorithm.Int.j.comput.Sci.Network,1:98-108

[5] Schildt,h,2010,The Complete Reference C 7th Edn.The McGraw-Hill Companies.New-York,NY,USA