ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Dual-layer Video Encryption & Decryption using RSA Algorithm

Swaleha N. Sayyad[1], Pramila S. Sutar[2], Rani S. Pise[3], Vidhya H. Raut[4], C.V. Nalawade[5]

B. E Student, Dept. of EnTC, S.B.Patil College of Engineering, Indapur, India[1,2,3,4],

Assistant Professor, Dept. of EnTC, S.B.Patil College of Engineering, Indapur, India[5]

ABSTRACT: Video encryption algorithm using RSA and Pseudo Noise (PN) sequence, aimed at applications requiring sensitive video information transfers. The system is primarily designed to work with files encoded using the Audio Video Interleaved (AVI) codec, although it can be easily ported for use with Moving Picture Experts Group (MPEG) encoded files. The audio and video components of the source separately undergo two layers of encryption to ensure a reasonable level of security. Encryption of the video component involves applying the RSA algorithm followed by the PN-based encryption.

KEYWORDS: MATLAB, RSA, GUIDE, PN Sequence , Encryption , Decryption , GUI

I. INTRODUCTION

Information security has traditionally been ensured with data encryption and decryption techniques. Different generic data encryption standards have been developed. Although these encryption standards provide a high level of data protection, they are not efficient in the encryption of multimedia contents due to the large volume of digital image/video data. For instance, enterprises with distributed locations having their business meetings via video conferencing, is now a commonplace. Having an intruder intercept the path of data- transmission and thereby gain access to the information being transferred can lead to horrendous situations especially in scenarios wherein sensitive data is being transferred. Another related domain is the video-on-demand application wherein certain privileged users are granted access to receive the benefits of the service. To ascertain that the signal is not intercepted on its transmission path and hence prevent the misuse of the service, encryption can be used.

II. LITERATURE SURVEY (Related work)

1 .Dual-Layer Video Encryption using RSA Algorithm
Aman Chadha, Sushmit Mallik ,Ankit Chadha, Ravdeep Johar
This paper proposes a video encryption algorithm using RSA and Pseudo Noise (PN) sequence, aimed at applications requiring sensitive video information transfers

2 .Video Encryption and Decryption using RSA Algorithm
Merlyne Sandra Christina C#1, Karthika M*2, Vasanthi M#3, Vinotha B*4
Security and privacy issues of the transmitted data have become an important concern in multimedia technology. To maintain balance between computational time and security, proposed RSA algorithm has been used to selectively encrypt and decrypt the sensitive video.

3 .Separable Reversible Data Hiding in Encrypted Image
Xinpeng Zhang
This work proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data.With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content.

4 .Digital Image Sharing by Diverse Image Media
Kai-Hui Lee and Pei-Ling Chiu
Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. The shares can appear as noise-like pixels or as meaningful images; but it will arouse suspicion and increase interception risk during transmission of the shares.

5 .RGB Based Secret Sharing Scheme in Color Visual Cryptography
M.Karolin1, Dr.T.Meyyapan2
Information hiding in the communication spectrum became a critical task. The Visual Cryptography is a type of cryptography that allows the image to be divided into multiple numbers of shares called transparent shares and then transmission of images. The intruder hence cannot understand the distorted image and thus the data communication becomes secured. In existing methods works for color images with 8 colors and even few of them without halftone Techniques

6. Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System
Somdip Dey, Asoke Nath, Shalabh Agarwal
Security and authenticity of data is a big challenge. To solve this problem, we propose an innovative method to authenticate the digital documents.

7. A visual cryptographic encryption technique for securing medical image
Aphetsi Keste
Confidential patient information over these networks. Digital encryption of medical images before transmission and storage is proposed as a way to effectively provide protection of patient information. Encryption before watermarking of these images is necessary in order to ensure inaccessibility of information to unauthorized personnel with patient.

8. An extended visual cryptography scheme without pixel expansion for Halftone image
N.Askari,H.M. Heys, and C.R. Moloney
Visual cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. In extended visual cryptography, the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual cryptography and biometric security techniques.

9. Fast and Secure Real-Time Video Encryption
Narsimha Raju, Ganugula Umadevi
Advances in digital content transmission have increased in the past few years. Security and privacy issues of the transmitted data have become an important concern in multimedia technology. In this paper, we propose a computationally efficient and secure video encryption algorithm.

10. A Proposal to Secure Visual Cryptographic Shares of Secret Image using RSA
Siddaram Shetty, Minu P. Abraham
This paper presents an approach to encrypt generated image shares of Visual Cryptography using Public key Encryption. We used RSA algorithm in order to provide the double security of the document. Hence, shares of secret image are not exist in their actual form for third parties (those who try to create fake shares) to make alteration.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

III. PROCESS DIAGRAM

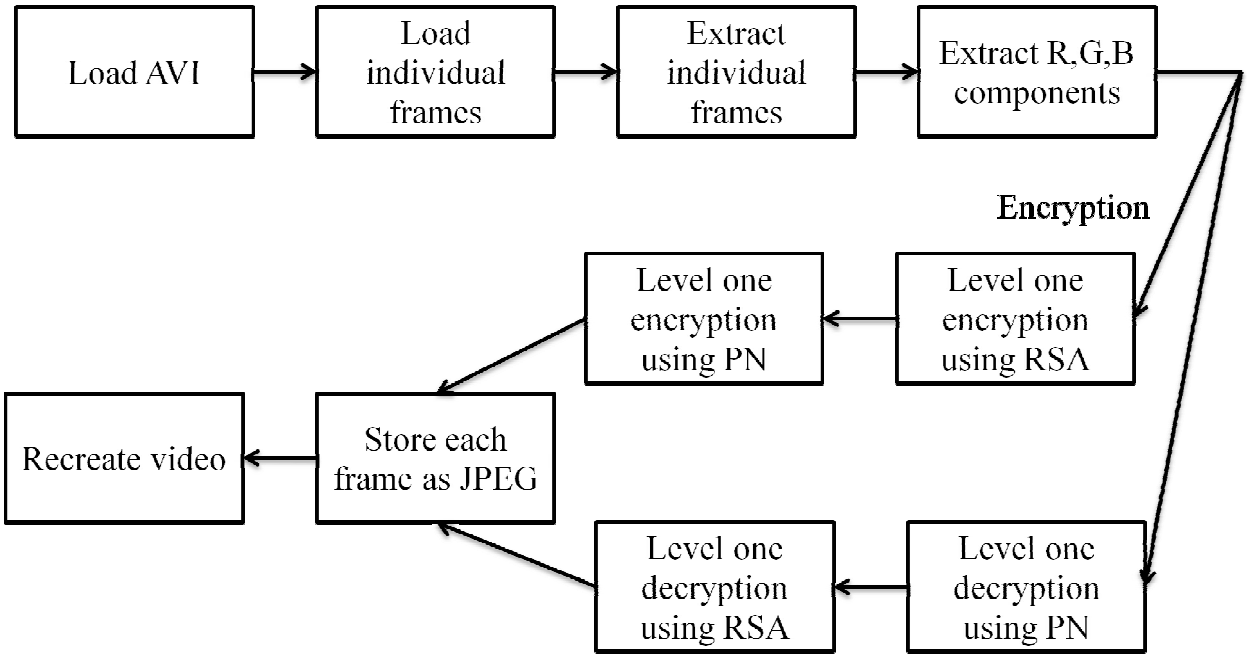

Fig.1 Process diagram of encryption and decryption

- Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those who possess the key to decrypt it.
- **Steps of Encryption:**

Step 1: The AVI file is loaded into the system.
Step 2: The frames of the file loaded, is extracted one by one.
Step 3: After the extraction process, the frames are loaded.
Step 4: The loaded frames are then segregated into their RGB components and the encryption takes place on the individual color components of the frame.
Step 5: The RGB frames are encrypted individually using the RSA algorithm.
Step 6: To initiate the RSA process, accept an input string from the user. The sum of the ASCII values of each character of the string input by the user is stored as x. Two large consecutive prime numbers are selected which are immediately next to x and pass them on as inputs to the RSA algorithm.
Step 7: Key distribution takes place.
(a) The public key is sent from the sender to the receiver.
(b) The receiver then sends a message M to the sender.
(c) The message M is first converted into an integer m, such that $0 < m < n$ by using an agreed-upon reversible protocol known as a padding scheme.
(d) The cipher text c is calculated corresponding to $c = m^e \pmod n$.
(e) The cipher text c is then sent from the receiver to the sender.
Step 8: The encrypted RGB components are then combined as a JPG file (with a frame number in the filename).
Step 9: Steps 3 to 6 for all frames are repeated for all the frames.
Step 10: The result is obtained after utilizing all the stored frames to create a video file with each stored encrypted image as an individual frame of the video.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

- Decryption: Decryption is the process of extracting the original message from a cipher text using the algorithm which requires a key to decrypt the message.

$$m = c^d \pmod{n}$$

- **Steps of Decryption:**

Step 1: The encrypted AVI video file is loaded into the system.
Step 2: The frames are extracted one by one.
Step 3: Each frame is loaded in the system.
Step 4: The RGB components are then extracted from the loaded frames.
Step 5: The RGB components are decrypted using RSA.
Step 6: The sender recovers m from c by using the private key exponent via computing m = cd (mod n).
Step 7: Each decrypted RGB component is then combined as a JPG file (with a frame number in the filename).
Step 8: Steps 3 to 6 are repeated for all frames.
Step 9: The result is obtained after utilizing all the stored frames to create a video file with each stored decrypted image as an individual frame of the video.

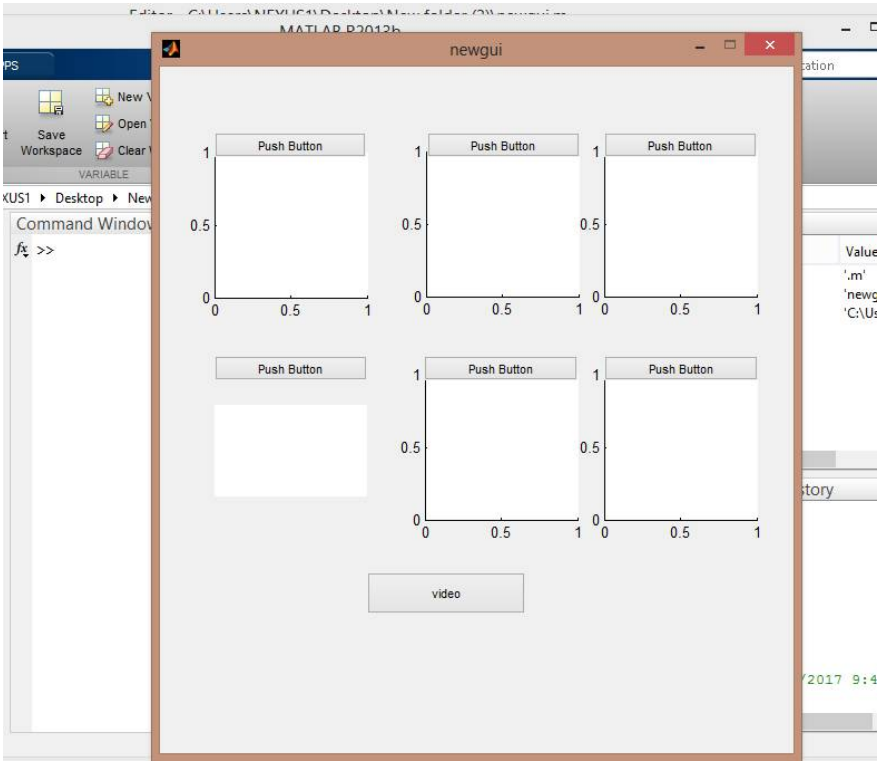

Fig.2 Before loading image

Above fig. Shows the Graphical User Interface before loading image . Using first push button we have to load the frame which is extracted from the video. Then we will encrypt the image using next push buttons and after that remaining push buttons are used to decrypt the image. At last we will get a original video.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

IV. PROPOSED ALGORITHM

RSA Algorithm:-
We propose a system using the RSA algorithm.

- RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977.
- It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, receiver can decrypt it using his own private key.
- **Steps of RSA Algorithm:-**

➢ Key generation,
➢ Encryption
➢ Decryption.

Key generation :- A key is a piece of information that determines the functional output of a cryptographic algorithm. Without a key, the algorithm would be useless. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption. There are two keys in RSA, i.e. Public key and Private key . The public key is known to everyone and is used for encrypting the messages; these messages can be decrypted only using the private key.

- Keys for the RSA Algorithm are generated in the following manner:

1) Select two distinct prime numbers p and q.
2) Compute: $n = p*q$
3) Compute: $\varphi(n) = (p - 1)(q - 1)$, where φ stands for the Euler's totient function.
4) Select an integer e such that $\varphi(n)$ and e are co prime.
5) Calculate d using the formula : $d = e^{-1} (\text{mod}\varphi(n))$.

- The public key consists of the modulus n and e (encryption exponent). The private key consists of the modulus n and d (decryption exponent), the decryption exponent has to be kept secret along with p,q and $\varphi(n)$, using which the decryption exponent can be calculated.

V. PSEUDORANDOM FUNCTION

Pseudorandom functions are like pseudo random generators whose output is exponentially long and it is such that given a seed, each bit of the output is computable. The security is against efficient adversaries that are allowed to look at any subset of the exponentially many output bits.

NEED FOR TWO LEVELS OF ENCRYPTION

Upon implementing RSA encryption for the video, the encrypted video turned out to visually resemble the original video, we can see it clearly in fig that the encrypted image bears some similarities to the original image. For highly sensitive data it is imperative that the encrypted video should not bear any visual resemblance to the original video. Hence, we try to remove any resemblance whatsoever from the encrypted video to the original video, to do this we propose the use of two levels of encryption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

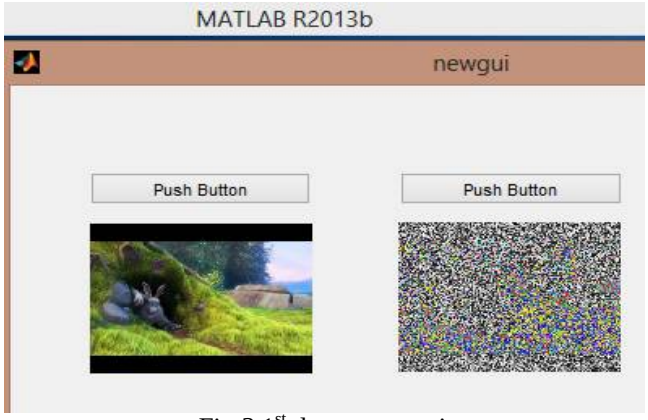

Fig.3 1st layer encryption

IN above figure we encrypt the image only once. From 1st layer encryption intruder will get sort of information so after 1st layer of encryption using RSA algorithm, we will encrypt it again using PN noise.

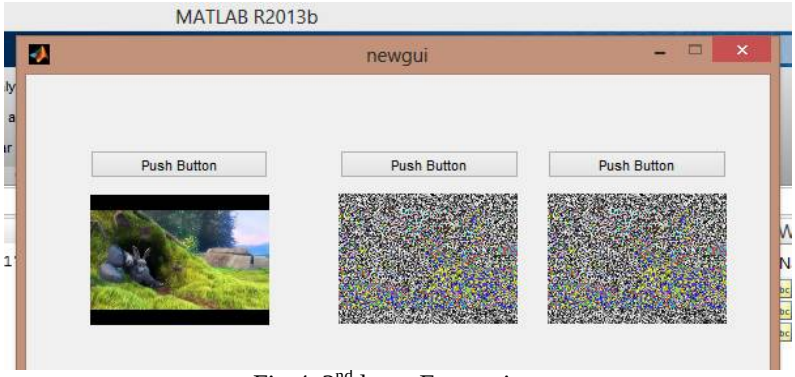

Fig.4 2nd layer Encryption

In this fig. 2 layer of encryption is takes place. From 2nd layer encryption there is any information will found to intruder.

We are sending key file and encrypted file via gmail.

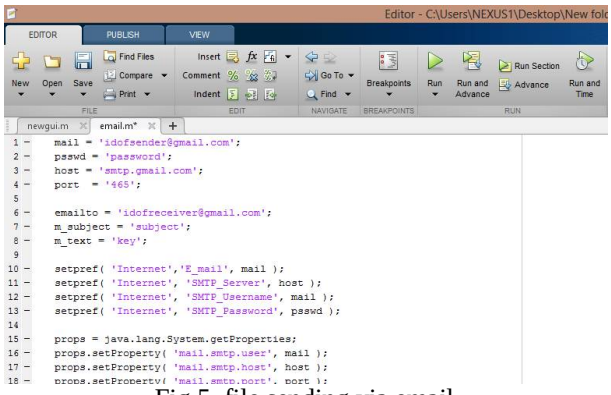

Fig.5 file sending via email

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

For extra level of security we use mail for sending key. It will be secure transmission because mail account will be accessed only by receiver. So only receiver can decrypt the video using that key .

VI. RESULTS

Here we get the original video after accepting the private from the sender . Key is send vai mail.

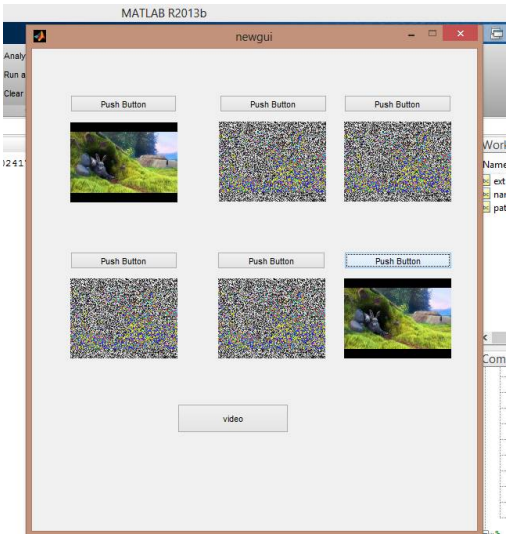

Fig.6 Overall encryption and decryption

Here is overall view of encryption and decryption. 2 layered encryption and 2 layer decryption is carried out. After that if we press push button for video then we will get original video.

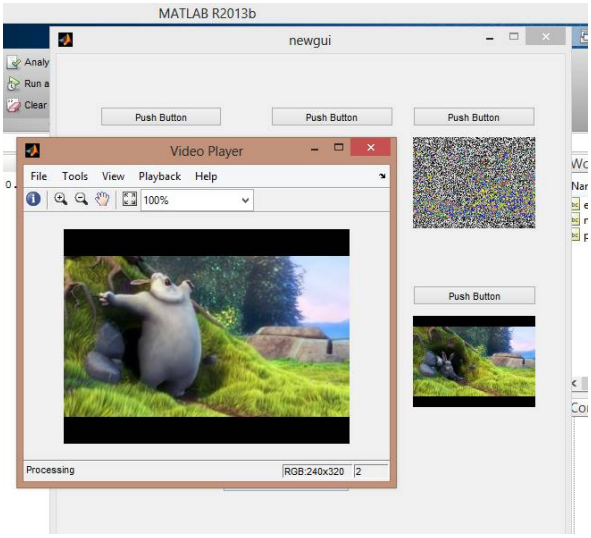

Fig.7 Video after decryption

Video is regained after decryption. Here we already saved the generated key in the programme to show overall process.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

VII. CONCLUSION

This system will help to secure the secret data from unauthorized use. New method of dual layer encryption methodology which enables to achieve zero visual resemblance and high security while not being severely penalized in Speed and Decryption ratio. The dual layer approach presents a promising approach to achieving a highly secure way of video encryption while not being very computationally intensive and time consuming.

REFERENCES

1. Aman Chadha, Sushmit Mallik ,Ankit Chadha, Ravdeep Johar, "Dual-Layer Video Encryption using RSA Algorithm " *International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015*
2. Merlyne Sandra Christina C#1, Karthika M*2, Vasanthi M#3, Vinotha B*4 , "Video Encryption and Decryption using RSA Algorithm", *International Journal of Engineering Trends and Technology (IJETT) – Volume 33 Number 7- March 2016*
3. Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image " , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012
4. Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media " ,
5. M.Karolin1, Dr.T.Meyyapan2 , "RGB Based Secret Sharing Scheme in Color Visual Cryptography ", *International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 7, July 2015*
6. Somdip Dey, Asoke Nath, Shalabh Agarwal , "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System ", International Conference on Communication Systems and Network Technologies,2013
7. Aphetsi Keste, "A visual cryptographic encryption technique for securing medical image ", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June (2013)
8. N.Askari,H.M. Heys, and C.R. Moloney, "An extended visual cryptography scheme without pixel expansion for Halftone image", 26th IEEE Canadian Conference Of Electrical And Computer Engineering,2013
9. Narsimha Raju, Ganugula Umadevi "Fast and Secure Real-Time Video Encryption ", Sixth Indian Conference on Computer Vision, Graphics & Image Processing
10. Siddaram Shetty, Minu P. Abraham , "A Proposal to Secure Visual Cryptographic Shares of Secret Image using RSA " International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 12, December 2014
11. Asha Bhadran R, " An Improved Visual Cryptography Scheme for Colour Images", International Research Journal of Engineering and Technology, Volume: 02 Issue: 05 | Aug-2015
12. Nentawe Y. Goshwe**, "** Data Encryption and Decryption Using RSA Algorithm in a Network Environment**",** International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013
13. *Mr. Praveen Chouksey, Mr.Reetesh.Rai,* "Secret Sharing based Visual Cryptography Scheme for color preservation using RGB Color Space", *International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 5, No5, October 2015*
14. Rima Saha, Shambhawi, Shray Maheshwari, Vijay Shankar Tripathi, " Enhancing Visual Cryptography using RSA Algorithm", International Journal of Research in Management, Issue 4, Vol. 3 (May 2014)
15. Siddaram Shetty1, Minu P Abraham, "**A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA**", International Journal of Innovative Research in Computer and Communication Engineering,Vol. 3, Issue 4, April 2015