IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue1)
Available online at: www.ijariit.com

Dual-Layer Video Encryption and Decryption using RSA Algorithm

C. V. Nalawade
E&TC (AP-Pune University)
chaitralip55@gmail.com

Swaleha N. Sayyad
E&TC(Pune University)
sayyadswaleha42@gmail.com

Pramila S. Sutar
E&TC(Pune University)
pramilasutar44@gmail.com

Rani S. Pise
E&TC(Pune University)
piserani@gmail.com

Vidhya H. Raut
E&TC(Pune University)
vidhyaraut86@gmail.com

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— RSA, GUIDE, PN Sequence, MPGA, AVI.

I. INTRODUCTION

Information security has traditionally been ensured with data encryption and authentication 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

a) Dual-Layer Video Encryption using RSA Algorithm
By 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

b) Video Encryption and Decryption using RSA Algorithm
By 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.

c) Separable Reversible Data Hiding in Encrypted Image
By 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 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.

d) Digital Image Sharing by Diverse Image Media
By 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.

e) RGB Based Secret Sharing Scheme in Color Visual Cryptography
By 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

f) Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System By
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.

g) A visual cryptographic encryption technique for securing medical image
By 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.

III. SYSTEM

In this system we are using following blocks

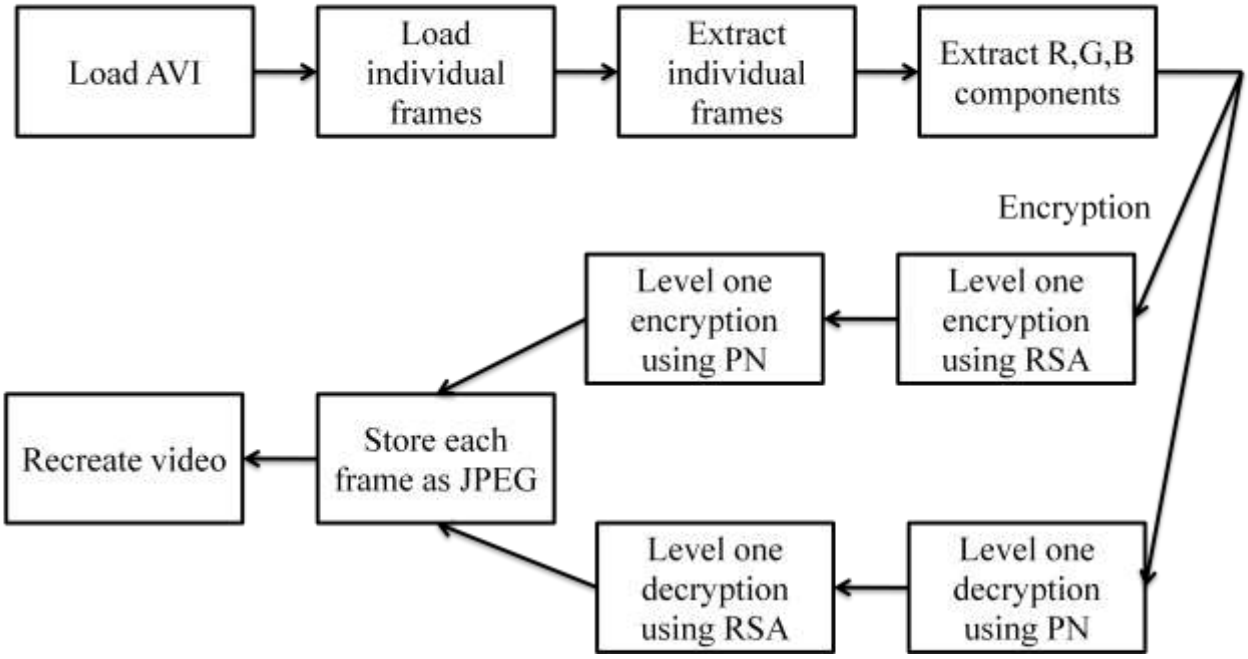

Load AVI
Load individual frames
Extract individual frames
Extract R,G,B components
Encryption
Level one encryption using PN
Level one encryption using RSA
Recreate video
Store each frame as JPEG
Level one decryption using RSA
Level one decryption using PN

Fig. Process diagram

IV. RSA ALGORITHM

We propose this system using 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

RSA algorithm consist of three stages

a) Key generation
b) Encryption
c) Decryption

a) 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.

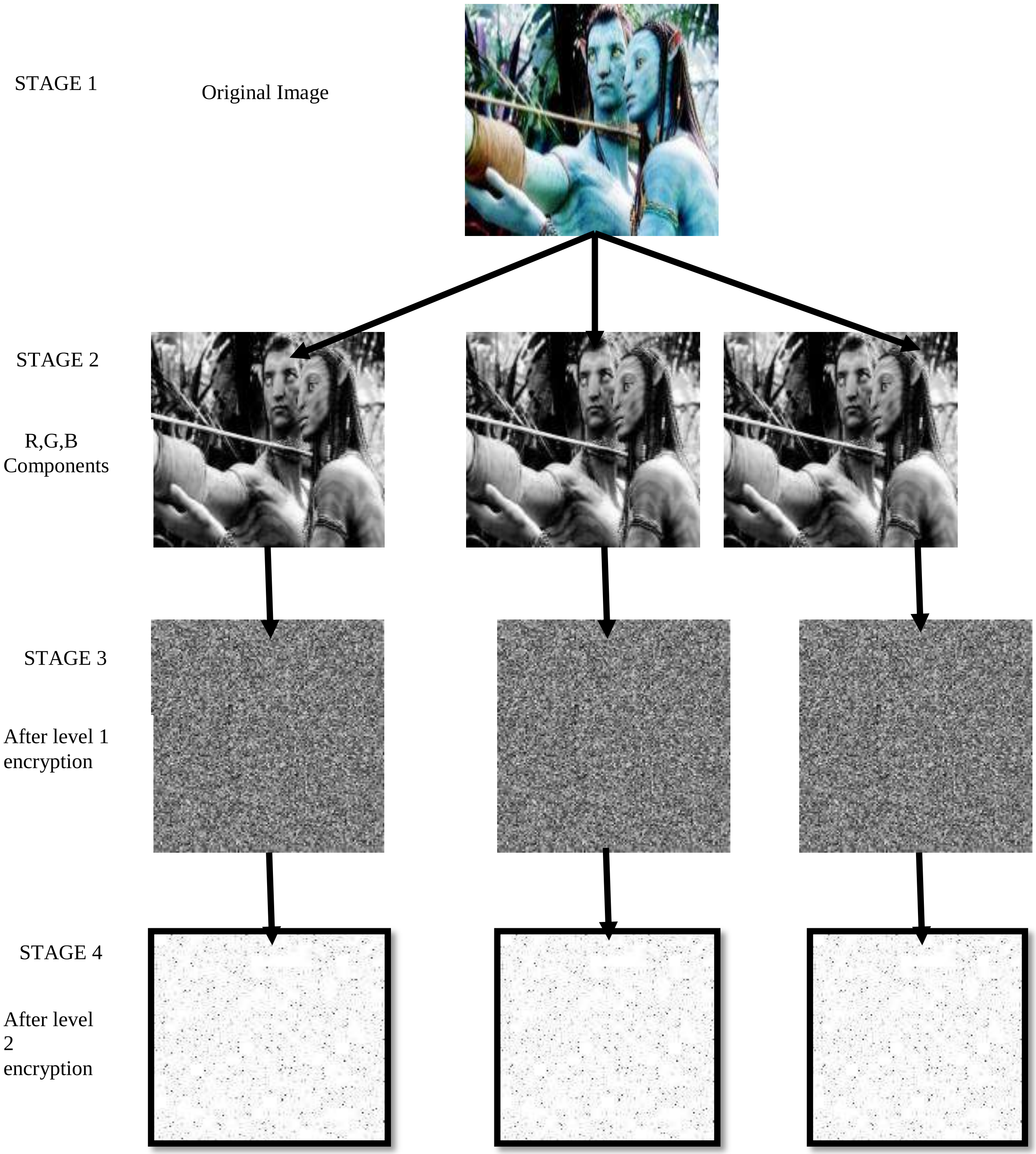
Keys for the RSA Algorithm are generated in the following manner:

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 : $d = e^{-1} (\mathrm{mod}\varphi(n))$

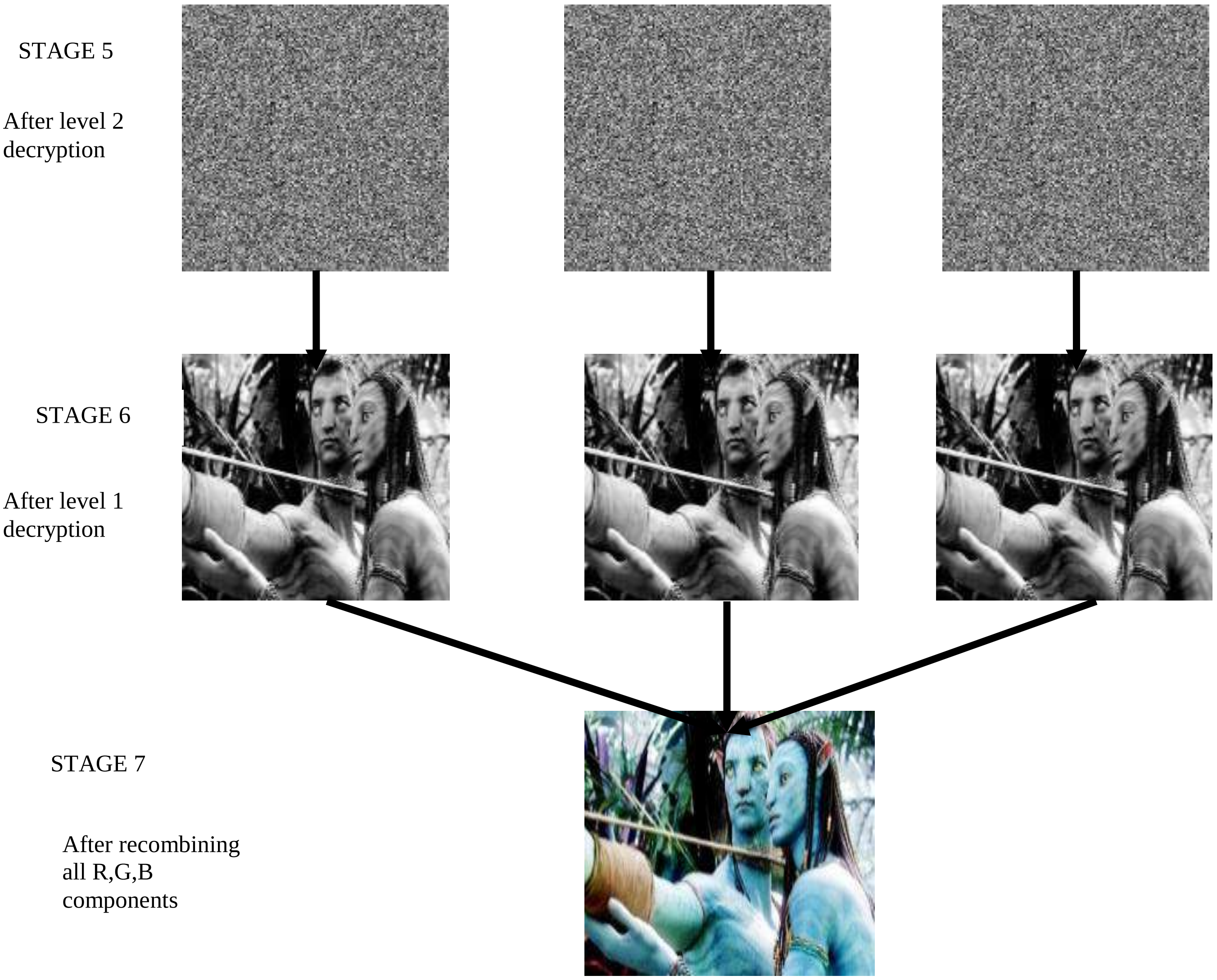
The public key consists of the modulus n and e (encryption exponent). The private key consists of the modulus n and d (decryption exponent), the decryption exponent has to be kept secret along with p,q and $\varphi(n)$, using which the decryption exponent can be calculated.

V. Expected result

Encryption stages:



Decryption stages:



Conclusions

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.

.

Acknowledgment

We are very thankful to our guide who has always helped us. Thanks to our college for providing us the best facilities and environment for research. Special thanks to our parents who has always been a source of inspiration for us.

References

[1] Aswathy Nair, Deepu Job, “A Secure Dual Encryption Scheme Combined with Steganography” International Journal of Engineering Trends and Technology (IJETT) – Volume 13 Number 5 – Jul 2014

[2] Vineeta Khemchandani, Kulvinder Kaur, “Securing Visual Cryptographic Shares using Public Key Encryption”.

[3] D. Kahn, “Cryptography Goes Public”, IEEE Communications Magazine, Vol. 18, 19–28, 1980.

[4] Kulvinder Kaur “Securing Visual Cryptographic Shares using Public Key Encryption” , 2013 3rd IEEE International Advance Computing Conference (IACC).

[5] D. Jena and S. Jena “A Novel Visual Cryptography Scheme”. 2008 IEEE DOI 10.1109

[6] Young-Chang Hou, "Visual cryptography for color images”,Journal of Pattern Recognition, Vol.36, pp.1619 – 1629, 2009.