Multilevel Security and its Application to Enhance Data Protection

Arush Kamboj
B.Tech (C.S.E.) IVth Year
School of Computing Science & Engineering, Vellore Institute of Technology, Vellore, India

Ravi Bisla
B.Tech (C.S.E.) IVth Year
School of Computing Science & Engineering, Vellore Institute of Technology, Vellore, India

N. Naveen Kumar
Assistant Professor
Department of Computer Science, VIT University, Vellore, India

ABSTRACT
A vast amount of information available on the internet along with the increased use of internet as a communication medium served a great deal in making the information available vulnerable. The number as well as the technique of attacks has become more and more sophisticated with time. This paper focuses on developing a multilevel security system (layers of cryptography combined with steganography) in order to achieve maximum security. The level of security is maximized by encrypting the information at different level and then using steganographic techniques to hide the information (be it a text or a multimedia file) inside multimedia file such as image, an audio file or a video file. The bits of a file are manipulated at each level. The change in the quality as well as size of the file is minimized by carefully choosing the unused area of the file or the least significant one. The paper explains this multilayered system by hiding an encrypted image, which further contains an encrypted text message, inside a video.

General Terms
Steganography, Cryptography, Encryption, Decryption, Security

Keywords
AES, LSB, DES

1. Introduction
Cryptography as well as steganography can be used to secure the sensitive or important information. While cryptography is the art of protecting information by transforming it into an unreadable format (called as, cipher) using the help of a password, known as secret key, steganography is completely different. It doesn't tamper with information or change it in any way. It is just a science of hiding information by embedding it in regular computer files (such as graphics, sound, text etc.). This hidden information can be a regular text message, a cipher or even an image.

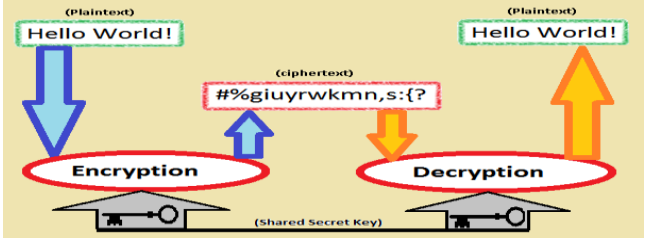

Fig 1: Basic model of Cryptography [Wikipedia]

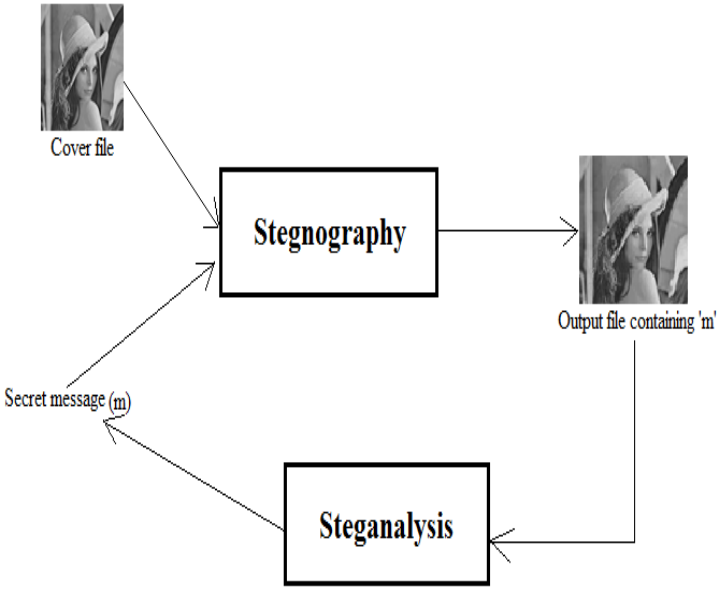

Fig 2: Basic model of steganography

The output file contains secret message hidden inside it. The output is almost exactly same as the cover file and hence attracts no suspicion. The secret message can be retrieved by applying algorithm exactly the opposite of what was being used to hide the message. The phenomenon is called steganalysis [1]. The cover file can be an image, audio or a video.

There are more than one way of hiding information inside another piece of information, steganography and digital watermarking. While cryptography and steganography complement each other as both are used to protect the information from unwanted attacks , watermarking is slightly different as it hides the information in a digital file so that the information is robust to alterations [2]. In addition it should impossible to remove the watermark without degrading the quality of the digital file. On the other hand, steganography hides the secret information in a carrier file so that the person will not notice the presence of information [2].

2. Related Work
There are a large number of steganographic techniques implemented to achieve secret communication. The main aim of steganography is to hide information in a carrier file so that a person cannot visibly deduce the knowledge of it. Steganography

can of two types viz. Linguistic and Technical. Linguistic is one where carrier media is text. On the other hand technical steganography offers a wide variety of methods such as Invisible Ink, microdots, computer based methods (uses redundant information in text, image, audio, videos) etc. It is nearly impossible to divide up all these methods. The authenticity of steganography is judged on the basis of three parameters such as capacity, robustness and security [4]. The steganographic approach used depends on the format of the carrier file.

3. PROPOSED WORK

3.1 Embedding Information

The proposed method is based on the image and video stegography combined complemented by AES algorythm for data encryption [5]. We have ecrypted the text before hiding the text inside the image and then we went on and ecrypted the image before hiding the image inside the main cover file (video). The flow chart of the process is shown in Fig 3. Below, the different levels of the system are explained in detail.

3.1.1 Level 1: Encrytpt Text message (AES Algorithm):

We used AES (Advanced Encryption Standard) algorithm to encryt the original message. The block size of AES is 128 bits but with different key lengths: 128, 192, 256bits. Unlike DES, AES is more secure and robust. AES is fast and requires low ram. So, after level-I we have a secure encrypted message, a cipher.

3.1.2 Level 2: Hide cipher inside the image:

In terms of computer language, an image can be represented as an array of numbers. These numbers are basically light intensities of pixels. Each pixel consists of a red, blue and green component each represent by 8 bits. Hence each pixel have 3 sets of values ranging 0 – 255 (24-bit = 8 bits for red, 8 bits for green and 8 bits for blue).

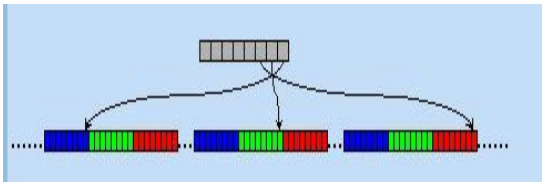

Fig 4: An array of pixels,each pixel containing 3 sets of values (8 bits each)

Various approaches have been designed to hide information in an image, most popular of which is LSB (Least Significant Bit) [6] where we modify the last bit of each pixel as it is considered to be least relevance.

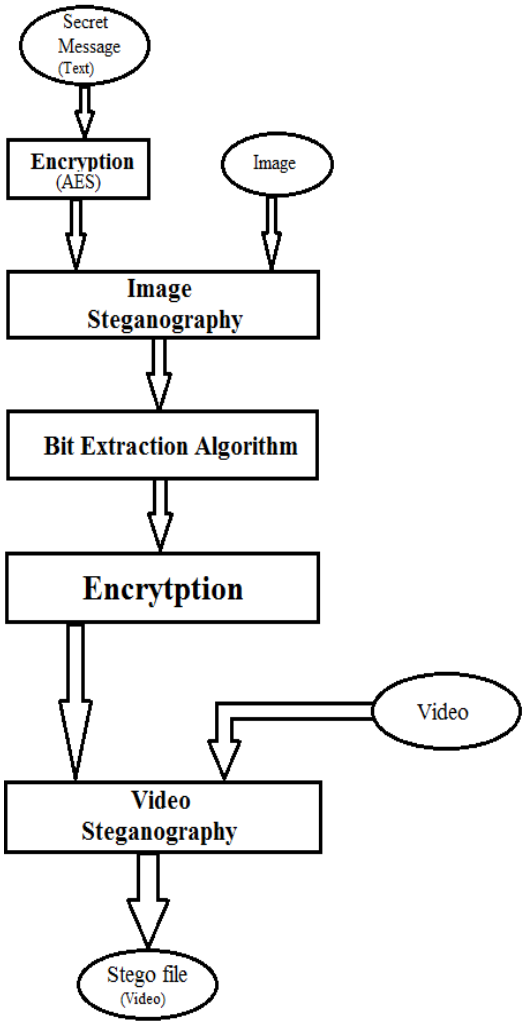

Fig 3: Basic Model of the proposed system

3.1.3 Level 3: Encryption of Image (By accessing the bits of the image)

As shown above in Fig. 3 each pixel has 3 sets of values stored in bits. Java provides various classes (WritableRaster, DataBufferByte, Graphics2D, ImageIO) to render the image pixel by pixel and thus storing the results in an array. Thus reading the input image stream by stream the pixels values are altered using an encryption algorithm (We used AES).

3.1.4 Level 4: Hide the encrypted image inside the carrier file (In our case, video)

Most common technique to transform a signal (Image or Video) from spatial domain to frequency domain is 2D DCT. DCT is used to separate the signal into parts of differing importance. The general formula to calculate the coeffient of DCT (S(u,v)) for a grid of pixels, which in our case is F(x,y), is given below [7]:

$$S(u,v)=\frac{2}{N}C(u)C(v)\sum_{n=1}^{N-1}\sum_{n=1}^{N-1}F(x,y)(\cos\frac{\pi u(2x+1)}{2N})*(\cos\frac{\pi v(2y+1)}{2N})$$

Where C(k) = $\frac{1}{\sqrt{2}}$ when k=0, otherwise C(k)=1

A video is nothing but a combination of high resolution images, called frames. In this step we collected the frames of the video and after collecting the frames secret information was embedded in the selected frame, say F, by applying DCT (Discrete Cosine Transform) on that channel under the alogrithm mentioned below:

***Input**: message, cover file*
***Output**: stego file*
while** data left to embed **do
get next DCT coefficient from cover file
if** DCT ≠0 and DCT ≠1 **then
get next LSB from message
replace DCT LSB with message LSB
end if
***insert** DCT into stego file*
end while

The following algorithm sequentially replaces the least-significant bit of discrete cosine transform (DCT) coefficients with message data.

3.4 *Extraction of Information*

Like the former proces, extraction of information is also done in four phases. This process is exactly the opposite process of the above.

3.2.1 Level 1: Steganalysis on stego file

Stego file here is the main output video file which contains encoded image. Encoded image hidden inside the stego file can be extracted by breaking the video in to frames and applying IDCT (Inverse-DCT) on each frame. The general formula to reproduce the grid of pixels F(x,y) is given below [7]:

$$F(x,y)=\frac{2}{N}\sum_{n=1}^{N-1}\sum_{n=1}^{N-1}C(u)C(v)*S(u,v)\left(\cos\frac{\pi u(2x+1)}{2N}\right)*\left(\cos\frac{\pi v(2y+1)}{2N}\right)$$

Where $C(k)=\frac{1}{\sqrt{2}}$ when k=0, otherwise C(k)=1

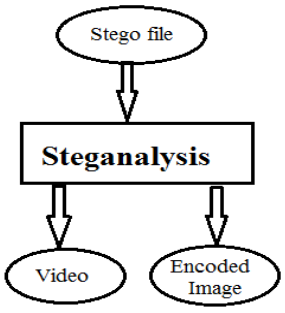

Fig 5: ***Steganalysis on stego file***

3.2.2 Level 2: Decrypting Encoded Image

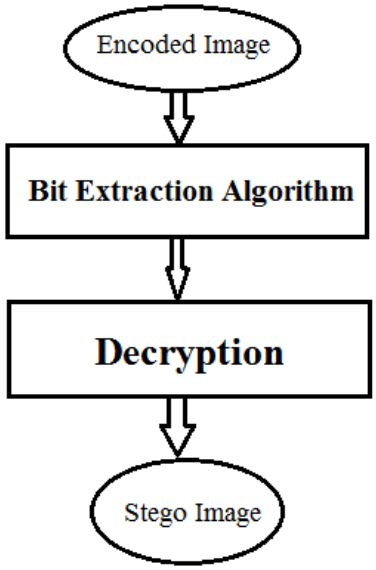

Fig 6: ***Decryption of encoded image***

The encoded image obtained by applying steganalysis is then decoded in the opposite fashion with which it was encoded. The result, called stego Image, is the orginal image used but with encoded message hidden inside it.

3.2.3 Level 3: Steganalysis on Stego Image

The encoded message (cipher) is then extracted from the stego image by applying steganalysis on stego image. The result of this process produced original image and the cipher (encoded secret message).

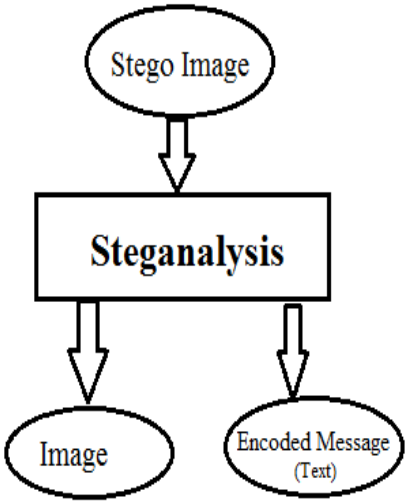

Fig 7*: Steganalysis on Stego Image*

3.2.4 Level 4: Decryption of the Cipher

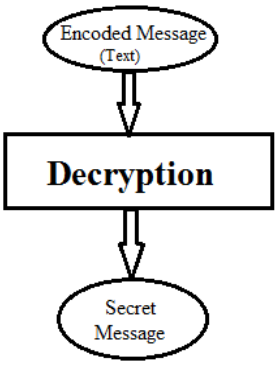

Fig 8 ***Decryption of the Cipher***

The cipher was then decoded to produce the original secret message intially used.

4. CONCLUSION

In this paper we discussed a multilevel process for hidind information in a file adding new security at each level. The proposed system uses AES for encrypting the text message and pixel values of image thus providing more security and robustness to the system. The system implement four levels of security and also encourages further research on adding more levels through the communication channel to achieve maximum security. We can conclude that proposed system is secure, robust and effective.

5. References

[1] Philip Bateman "Image steganography and steganalysis" (2008 August)

[2] Vandana Thakur and Monjul Saikia, "Hiding Secret Image in Video" IEEE Internet Computing, Vol. 9,

[3] Vipula Madhukar Wajgade and Dr. Suresh Kumar, "Enhancing Data Security using Video Steganography," IJETAE, Volume 3, Issue 4, April 2013

[4] B.Dunbar.A Detailed look at steganographic techniques and their use in an Open-Systems Environment,Sans Institute,1(2002).

[5] Sanket Upadhyay, Priyanka pimpale and Rohan Rayarikar, "SMS Encryption using AES algorithm on Android", IJCA(0975 – 8887)Volume 50– No.19, July 2012

[6] Hiding Image in an Image using LSB Method by Deepesh Rawat and Vijaya Bhandari, International Journal of Computer Applications (0975 – 8887) Volume 64– No.20, February 2013

[7] Dct Based Image Steganographic Approach by Sonawane Viraj, Mali Jagdish and Prof.R.N Awale Vol. 3, Issue 4, Jul-Agu 2013, pp. 381-384

[8] L. Y. POR, B. Delina "Information Hiding: A New Approach in Text Steganography" 7th WSEAS Int. Conf.

[9] Monika Aggarwal "Text steganographic approaches: A comparison" , IJNSA, Vol. 5. No.1, January 2013

[10] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles and Maricel O.Balitanas "Data hiding in a video" IJDTA Vol 2, No. 2 June 2009

[11] A. Swathi, Dr. S.A.K Jilani, Ph.D " Video Steganography by LSB Substitution Using Different Polynomial Equations" IJCER Vol 5 Issue 5

[12] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav "Steganography Using LSB" IJERA Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

[13] Shailender Gupta, Ankur Goyal, Bharat Bhushan "Information Hiding using LSB Steganography and Cryptography"

[14] http://binary-universe.net/index.php?article=3&language=e and article=3

[15] http://stackoverflow.com/questions/3018086/simple-basic-steganography-algorithms-and-methods

[16] http://www.nbcnews.com/tech/security/internet-speeds-are-rising-sharply-so-are-hack-attacks-n87616

[17] http://scien.stanford.edu/pages/labsite/2005/psych221/projects/05/vvikram/stego.htm

[18] http://www.citi.umich.edu/u/provos/papers/practical.pdf

[19] http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.208.5195