Proceedings of the International Conference on
Information Security ICIS'05,
Pondicherry Engineering College, Pondicherry, India. Dec.7-9,2005, pp.1 -6.

Dual Level Data Encryption Using Image Segmentation And AES For Combating Piracy

Dr. M.C Govil[1], Pranav Agrawal[2], Sushrut Chelawat[2]

[1]*Department of computer Engineering,MNIT Jaipur*
[2] *Department of Electronics Engineering, MNIT Jaipur*

Abstract

We propose a new method for combating software piracy by using a highly secured AES algorithm and image segmentation method. Integrating two methods along with the use of the hardware profile of the computer makes the keyless distribution of the software a reality, where the image itself acts as a key. The method proposed could also be used for the secure transfer of the data.

1. INTRODUCTION

Hardware profile of a computer is unique, so it is used as the key by the vendors while distributing their product.Using the hardware information of the client, a particular key is generated and that key is given to the client. So when the installer program tries to install on the client computer it asks for that particular key which the vendor has given to the client. After entering the key installer program internally generates the key, depending upon the computer on which installation is taking place. It then matches the key with the entered key and proceeds if that key matches.

Now, our idea is to store the encrypted form of the hardware profile of the client computer in an image and gives the image to the client along with the software. When the installer programs tries to install the software on the client computer it extracts the hardware profile from the image then matches with the hardware profile of the computer on which it is trying to install

It is advantageous from the former in the following aspects:

1) Instead of the particular key, an image is given which is a far more secure way of transferring the information.

2)We are implementing double level security by as first encrypting the hardware profile using AES algorithm and then hiding the data into the image by using segmenting method (elaborately described in the later part).

3)We develop two DLL's; one for encryption and another for decryption, as encryption DLL is only with the vendor and the decryption DLL and the encrypted image will be given to the client.

4) We are using the random function to generate the key for the DES algorithm and the parameter used to generate the key using random function is also stored in the image, so when the decryption of the image is taking place it extracts the parameter from the image the again acts as the input to the to the random function, which again generates the same key, which was generated at the time of encryption as the algorithm of generating random function is same both at the encrypting end as well as the decrypting end. So it again makes the cryptanalysis very difficult.

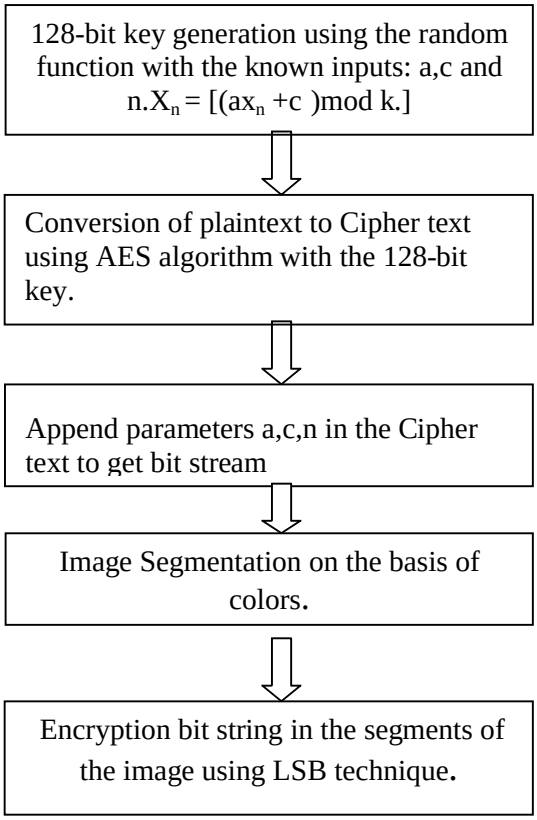

Fig. 1: Algorithm

2.1 RANDOM KEY GENERATION

To generate a sequence of random numbers, randomness and unpredictability are essential elements. We employ pseudorandom number generators (PRNG's) technique, which follow :

Xn = [(axn +c) mod k.]

a,c,m and Xo are known parameters

Generally m is kept large to increase the number of unpredictable sequences.

The Blum Blum Shub Generator is used:

n=pq (p and q are big prime numbers)

$Xo=S^2 \bmod n$

For i=1 to infinity

$Xi=(Xi-1)^2 \bmod n$

Bi =Xi mod 2

2.2 AES

Advanced encryption Standard (AES) utilizes a 128 bit key and hence to crack this encryption is a Herculean task.

The cipher text creation involves the sequential combination of shifting rows, mixing columns and round key shifting.

The 128-bitkey is generated using step 1 is used to encrypt the 16 byte long plaintext thus generating a new bit pattern to be put into the image.

Also we append the parameters like a,c,m and Xo with the cipher text obtained.

2.3 IMAGE SEGMENTATION METHOD

The basic motive behind using this technique is to make the cryptanalysis of the image difficult. If one goes for the common techniques like LSB or MSB encryption techniques, the main disadvantage associated with the above methods is that if the values of the pixel is viewed then the data can easily be extracted if the concerned pixel is compared with its neighboring pixels as it will be having the different value from its neighboring pixels.

Our approach to solve this problem is to hide the information in the different segments of the image. Image could be modeled as the summation of the different color segments. If we decrease the range of color for the selection of segments then the maximum segments can go up to total number of pixels in an image.

$$M=\sum_{p=1}^{m} \sum_{i=1}^{nm} S_{ip}(C_p , R_{ip})$$

Sip denotes the ith segment of the image having the Cp color range and Rip location in the image.
Cp ={[R,G, B]minp,[R, G, B]maxp}
Let nm be the number of segments present of color m
Rip region is the set of the points lying in the range of Cp of (i, p) region

Four extreme co-ordinates of the region is in two directions one vertical and another horizontal
Extreme horizontal co-ordinates are :
(Xmin , Y1), (Xmax , Y2)
Extreme vertical co-ordinates are :
(X1,Ymin),(X2, Ymax)
So any point lies in the region is the concerned point, as shown by the gray color in the Fig. 2.

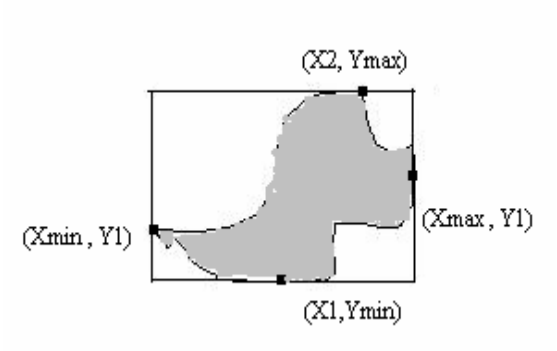

Fig. 2: Segmented Unit

First from the image different segments of a particular color range is selected and then the LSB of the pixels corresponding to those of the selected segments are changed according to the data, so for a particular segment which is selected, all the pixel values are changed uniformly according to the stream of data.

To make the encryption more secure one can hide the data by randomly selecting the color regions of the image and then hiding the data in the region.
We have used the above mention technique and taken the group photograph from which the segments are selected on the basis of the skin color.

For e.g. if the data to be hidden is 101…, the LSB of all the pixel values of the first segment is made '1' and LSB of all the pixel values of the second segment is made '0' and so on.

2.4 DETERMINATION OF THE RANGE OF SKIN COLOR

We took the group photographs for the encryption, so there was the need to determine the range of skin color. It is well known fact that the RBG color model is not a reliable model for detecting skin color. A different model of skin color is used: the YIQ model, adopted by NTSC for color television broadcasting. The conversion of RGB to YIQ components is done using the following formula:

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.275 & -0.320 \\ 0.212 & -0.523 & 0.311 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

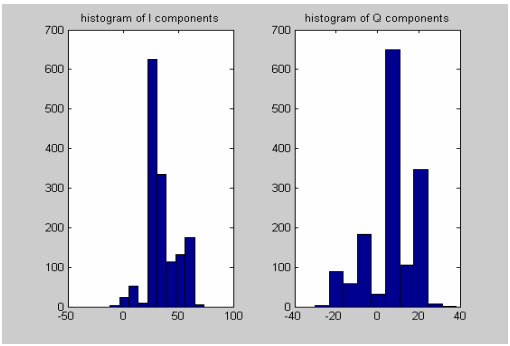

Fig. 3 .Histogram of I and Q components in YIQ color space

YIQ represents color in terms of its luminance (Y), and hue and saturation (I and Q). I and Q correspond approximately to the amounts of blue and red in the color. Given appropriate thresholds, YIQ can be effectively used to identify skin regions

Similarly the approximate threshold for other colors can be determined by plotting the histograms. However we have used only the segments of skin color.

2.5 ENCRYPTION OF TEXT INTO THE IMAGE

Once the range of skin color is determined each pixel is put through the YIQ threshold, and the resulting mask image is obtained having the segments shown by white color. Then each segment is selected one by one and then the pixel value of point of the segment is changed according to string which includes cipher text and the parameters for the key generation at the decryption end.

3.0 CONCLUSION

Thus the system is efficient. If brute force technique is employed to get into the data, it would take around 5.4×10^{18} Years. With an additional level of encryption added the cryptanalysis would be impossible.
The piracy would end as the license authentication is unique to every computer. On the –fly key generation and encryption would be a salient feature.

REFERENCE

[1] Matlab Implementation of the Advanced Encryption Standard J¨org J. Buchholz http://buchholz.hs-bremen.de December 19, 2001

[2] Cryptography and network Security, Pearson education, William Stallings..