CRYPTOGRAPHIC STEGANOGRAPHY

Vikas Yadav[1] Vaishali Ingale[2] Ashwini Sapkal[3] and Geeta Patil[4]

[1]ZS Associates, Pune, India
gunwalvikas@gmail.com
[2,3,4]Department of Information Technology, Army Institute of Technology, Pune, India
[2]vaishalidharkar@gmail.com, [3]ashwini.sapkal@gmail.com, [4]geetapatil34@gmail.com

ABSTRACT

In the cryptographic steganography system, the message will first be converted into unreadable cipher and then this cipher will be embedded into an image file. Hence this type of system will provide more security by achieving both data encoding as well as data hiding. In this paper we propose an advanced steganocryptic system that combines the features of cryptography and steganography. In this proposed steganocryptic system we will encrypt the message into cipher1 by using Kunal Secure Astro-Encryption and we again encrypt this cipher to cipher2 by using grid cipher technique. Advantage of Kunal Secure Astro-Encryption is that it generates random useless points in between, thus fixed size messages can be generated providing more security compared to other cryptographic algorithms as the number of characters in original message cannot be found from encrypted message without the knowing the black holes. Now we will embed this cipher2 into image file by using visual steganography .In this proposed steganocryptic system we will use modified bit insertion technique to achieve visual steganography. This proposed system will be more secure than cryptography or steganography techniques[digital steganography] alone and also as compared to steganography and cryptography combined systems.

KEYWORDS

kunal astro secure cryptography, grid computing, modified bit insertion technique, LSB insertion technique

1. INTRODUCTION

1.1 Overview of kunal astro secure cryptography:

In kunal astro secure cryptography method [1] we assign a unique set of coordinates, known only to receiver and sender. Another set of points known as should also be shared only between the sender and receiver.

The next step is to calculate the ASCII equivalent of each character in the message and add it with any multiple of the range of ASCII characters. Let's call this value d

Then we plot a point on the sphere with any star chosen at random from given stars and radius d. The point is plotted by taking any random value of θ and φ.

Sundarapandian et al. (Eds) : CCSEIT, DMDB, ICBB, MoWiN, AIAP - 2014
pp. 17–23, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4803

We check if this point lies inside or on any black hole or the point is already in the cipher text. If it does then we regenerate the point by going back to step involving generation of point.

We now check if this point is closest to the star from which it is generated in comparison to other stars. If not, then we regenerate the point by going back to step involving generation of point.

Now we round up the point to 2 decimal places and remove the decimal point. Now The message is further compressed by converting this number from base 10 to base 100 and append it in cipher text by separating the coordinates with a comma.

To decode it, first retrieve the triplet from cipher text each of which is separated by comma. Then we decompress it by converting from base 100 to base 10 and divide each number by 100. This will be the x, y and z values of the point.

Check if this point lies on or inside a black hole, if it does then generate nothing.

If it does not come in or on a black hole then find the star closes to this point and the distance of that star from this point. Round off this distance to nearest whole number. Take remainder by dividing this rounded distance with the maximum range of ASCII characters. This remainder is the ASCII equivalent of plain text character. Convertthis ASCII value to character to get the plain text.

The entire coordinate system has origin which is shared just between the sender and receiver.

1.2 Overview of steganography

Steganography [5] is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

There are various methods of steganography[5] e.g. Sound Technique ,Video Technique, Image hiding, Binary File Technique .In our proposed method we are going to implement Image Steganography[4][8] .The bit insertion technique is the most common technique used in image steganography ,in bit insertion technique the LSB of a pixel can be modified.

Reference [4] explains various other techniques. Many examples of LSB scheme can be found is ref [7].

1.3 Grid Cipher

It is a way to send secret messages. In grid cipher two coordinates of numbers will stand for a letter. For example, in the figure given below 68 is encrypted as ‘>‘.we can also do encryption in reverse way, like letter ‘B’ can be encrypted as ‘’86’.

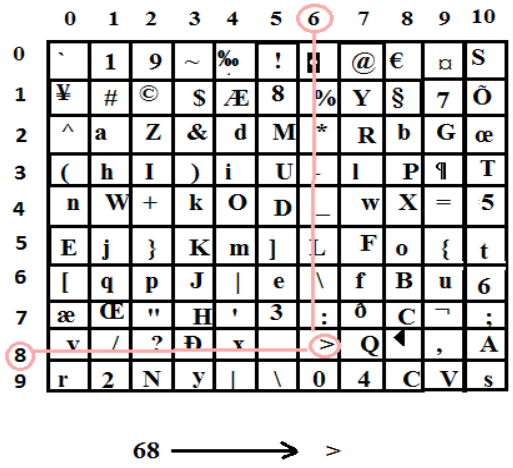

Figure 1. Grid Cipher

In our proposed system we will be having a grid database. From that grid database we will select a reference grid (this can be selected by using image properties, like depending upon width and height or it can be selected by referring size of image file or text file).Now from that reference grid(reference grid will be a collection of grids) we will select one grid (matrix) to encrypt our text.

If the total no of digits in the cipher text are odd then we will make use of our 10^{th} column of grid cipher to get cipher2 text. For example suppose our cipher text is 687 (odd number of digit) then we can decode 68 as '>' (refer figure 1) and 7(the single digit left) can be decoded as 7^{th} row of 10^{th} column i.e. ';' (refer figure 1).

Hence 687 can be decoded as '>;'.

1.4 Modified Bit insertion Technique :

In modified bit insertion technique we will first truncate the pixel values i.e. R,G,B values of a pixel to a predefined digit(for example, we can truncate the pixel values to the nearest zero digit)

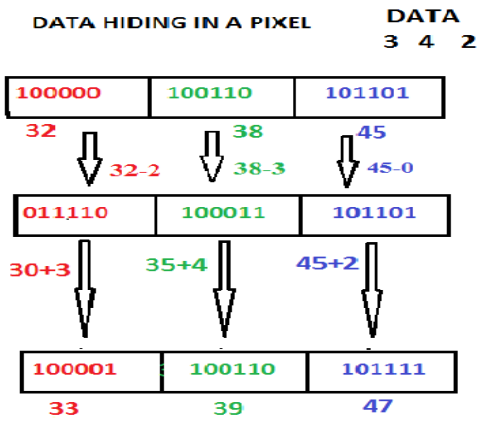

Figure 2. Modified Bit Insertion

For example, In above figure 2 first pixel value is truncated to nearest multiple of 5 and after than data is embedded. Thus the deviation in the R,G and B value of a pixel after storing the data is very less as compared to simple LSB insertion technique. Hence distortion in the image will be very less as compared to LSB insertion technique. And another advantage is that there is no need to send original image to the receiver (we have to send original image with stegano image so that receiver can decode the data from stegano image by pixel based image comparison[6] with original image).

2. THE PROPOSED METHOD

2.1 Message encryption

Step 1: We will encrypt our message by using kunal astro secure encryption into a cipher text.
Step 2: Now the cipher text obtained in step 1 is again encrypted by using matrix cipher(grid cipher technique) into cipher2 text.

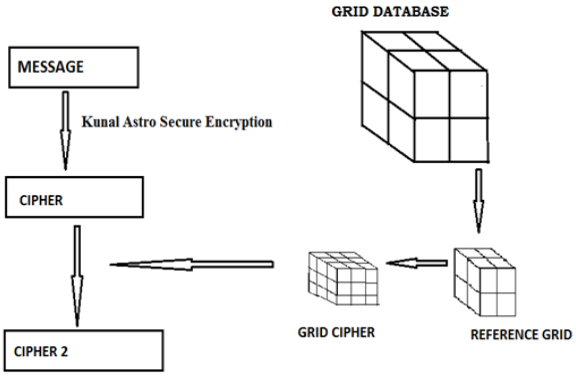

Figure 3. Message Encryption

2.2 Cipher hiding

Now we will hide the cipher2 text into an image file by using modified bit insertion technique. We will hide 1 byte of data per pixel. Here the cipher2 text file should not be too large. Amount of data that can be embed is depends on the image file. In large size file we can embed large amount of data . the cipher hiding in pixel can be understood by the figure 4.

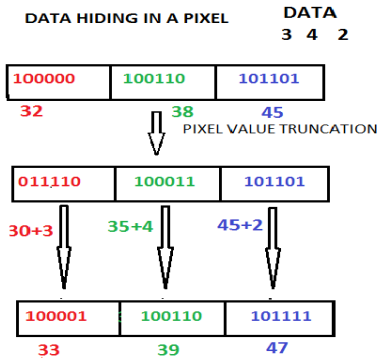

Figure 4. Cipher Hiding

2.3 Retrieval of cipher

Now we can extract the cipher2 text from our image file by the shown in the figure5 below. By doing so we will get cipher2 text.

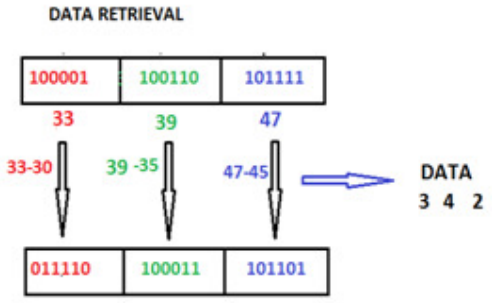

Figure 5. Retrieval of Cipher

Now just by performing reverse steps as that of encryption we can decrypt the cipher text into our plain text message. Firstly we will decrypt the cipher2 text into cipher text and now this cipher text can be decrypted to plain text message by using kunal secure astro encryption. Figure 6 shows the decryption of cipher2 into cipher text and cipher into our message.

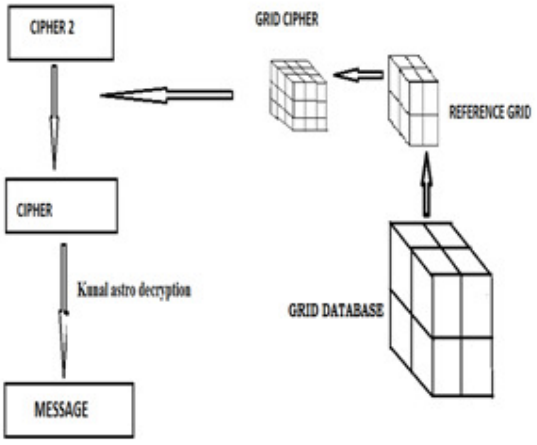

Figure 6. Decryption of cipher

3. ADVANTAGES AND APPLICATIONS

1. This method will provide more security to the information being transmitted than any other cryptographic or steganographic system as it combines both the features.

2. Extra level of security can be achieved by using grid cipher encryption

3. Distortion in the final multimedia image will be very negligible as we are using modified bit insertion technique.

The proposed system is applicable to the following areas :

1. Confidential communication and secret data storing.
2. Protection of data alteration.
3. Access control system for digital content distribution.
4. Media Database systems.

4. FUTURE SCOPE

This method can be used to increase the security on web based applications. The user will be asked to provide the secret key and the password can be compared from image files using the key. It can be used as advancement over the existing option to input the security phrase in various web based applications

REFERENCES

[1] Kush Jain, Vaishali Ingale and Ashwini Sapkal (2013) "Kunal Secure Astro-Encryption- Data Encryption and Compression Using Planar Geometry", IJETCAS.
[2] Mizuho NAKAJIMA (2002) "Extended use of Visual Cryptography for natural images, Department of Graphics and Computer Sciences", Graduate School of Arts and Sciences, The University of Tokyo.
[3] Bart Preneel (1997) "Cryptographic Algorithms: Basic concepts and application to multimedia security", Katholieke University, Belgium.
[4] T. Morkel (2005) "An Overview of Image Steganography", Department of Computer Science, University of Pretoria, South Africa.
[5] G F. Johnson and S. Jajodia (1998) "Exploring steganography: Seeing the unseen," IEEE Computer Mag., pp. 26–34.
[6] Paresh Marwaha, Piyush Marwaha and Shelly Sachdeva (2009) "Content based Image Retrieval in Multimedia Databases", International Journal of Recent Trends in Engineering .
[7] R. van Schyndel, A. Tirkel, and C. Osborne (1994) "A digital watermark," in Proc. IEEE Int. Conf. Image Processing, vol. 2, pp. 86–90.
[8] Elvin M. Pastorfide and Giovanni A. Flores (2007) "An Image Steganography Algorithm for 24-bit Color Images Using Edge-Detection Filter", Institute of Computer Science.
[9] Debashish Jena (2009) "A Novel Visual Cryptography Scheme" IEEE International Conference on Advanced Computer Control.

AUTHORS

Vikas Yadav received the BE Information Technology degree from Army Institute of Technology, Pune in 2014. he is now working in ZS Associates as a Business Technology Associate (BTA). His research interests include Security, Database

Prof Vaishali S. Ingale received the ME Computer degree from Pune University in 2008. She is now working as Assistant Professor in Army Institute Of Technology. Her research interests include Security, Algorithms, Cloud and Artificial Intelligence.

Prof. Ashwini T. Sapkal received the B.E. computer science and Engineering and Master's degrees from M.G.M's College of Engineering, Nanded, India in 2002 and Vishwakarma Institute of Technology, Pune, India in 2010, respectively. she is currently pursuing the Ph.D. degree with the Shree Guru Govind Singh Institute of Engineering and Technology, Nanded, India. She is now working as an Assistant Professor in Army Institute of Technology, Pune, India. Her current research interests include Neural Network, Pattern Classification algorithms and Cryptography.

Prof Geeta D. Patil received the ME Computer degree from College of Engineering Pune, India in 2008. She is now working as Assistant Professor in Army Institute Of Technology. Her research interests include Security Algorithms, Embedded Systems .