National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)
Proceedings published in International Journal of Computer Applications® (IJCA)

Enhancing the Impregnability of Text Messages at Multiple Levels

S. Gurusubramani [1], T. Prabahar Godwin James [2,] Venkatesh[3]

-[1] Assistant Professor (Gr – II), MCA Department, Sri Sai Ram Engineering College, Chennai,
- [2] Assistant Professor (Gr – II), MCA Department, Sri Sai Ram Engineering College, Chennai,
- [3] Student, II MCA, MCA Department, Sri Sai Ram Engineering College, Chennai,

ABSTRACT
In the field of Data Communication, security-issues have got the top priority. The degree of security provided by a security tool has become the main evolutionary criteria. There has been an ample of security tools to protect the transmission of multimedia objects. But approaches for the security of text messages are comparatively less. Classical Cryptography is one of the ways to secure plain text messages. The proposed model combines cryptography, steganography with an extra layer enforcing security. This newly introduced layer imposes the concept of secrecy over privacy. The Proposed System has an additional level of security. In this project the concept of Multi Layer Data Security (MLDS) has been introduced. For encryption and decryption, a mathematical operation called Multiplicative Modulo (MM) has been used in between the text and the generated keys. Here, the concept of Cryptography and Steganography (as two Layers of Security) and in between them an extra layer of security is introduced.

The two new methods namely Code Matrix Mapping and Matrix Pix Mapping (MPM) are used to employ the above mentioned extra security layer. This newly introduced extra layer of security changes the format of normal encrypted messages and the security layer followed by it embeds the encrypted messages behind multimedia cover object. In the first layer of security, the original text message is encrypted by applying a function involving mathematical operations. In the second layer, the encrypted code is converted into binary matrix by a Mapping method. In the third layer of security, the matrices obtained above are mapped into pixels of an image.

Keywords
LSB, RGB, DP, MLDS, IDE, MPM, ASCII, MM

1. INTRODUCTION
The IT **industry** is witnessing many physical and technological changes leading to consolidations, reformation and also reorganizing the way in which the business is done. The use of leading edge technology to precisely assess the requirements of the business, and proficiently and successfully implementing a solution is a critical part of building competitive advantage.
Along with data transmission, security is also implemented by introducing the concept of steganography, watermarking, etc. In this type of combined approach there exits some disadvantages. In remote networking, at the time of transmission on hidden encrypted text message, if the snoopers get the track of the hidden text, then they could easily get the encrypted text.
Now breaking of encrypted code can be achieved by applying some complex mathematical operation. So, there remains some probability of snooping of information. So, this type of techniques requires another level of security which can route the Cryptanalyzer or Steganalyzer in a different direction.
This paper represents a heuristic approach to introduce the concept of Multiple levels of Data Security in the field of combined Cryptography and Steganography. It has three layers of security, code generation & encryption using public key, code matrix mapping and matrix pix mapping.
This work is specifically focused on protection of any information which is in the form of text. The design of this technique is based on extensive analytical as well as experimental modeling of the data-hiding process.

1.1 Steganographic systems
The most of today's steganographic systems use images as cover object because people often transmit digital images over email and other communication media. Several methods exist to utilize the concept of Steganography as well as plenty algorithms have been proposed in this regard. To gather knowledge in this particular research field, we have concentrated on some techniques and methods which are described below.
Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover object. For images as a covering media, the LSB of a pixel is replaced with an M's bit. If we choose a 24-bit image as cover, we can store 3 bits in each pixel by modifying the LSBs of R, G and B array. To the human eye, the resulting stego image will look identical to the cover image.
Hiding data in the features of images is also an important technique which uses the LSB modification concept. In this method, to hide data in an image the least significant bits (LSB) of each pixel is modified sequentially in the scan lines across the image in raw image format with the binary data. The portion, where the secret message is hidden is degraded while the rest remain untouched. An

attacker can easily recover the hidden message by repeating the process.

A steganography system is designed for encoding and decoding a secret file embedded into an image file using random LSB insertion method. In that method, the secret data are spread out among the cover image in a seemingly random manner.

The key used to generate pseudorandom numbers, which will identify where, and in what order the hidden message is laid out. The advantage of this method is that it incorporates some cryptography in that diffusion is applied to the secret message.

The next interesting application of steganography is developed by, where the content is encrypted with one key and can be decrypted with several other keys. In this process, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information.

In 2007, an algorithmic approach to obtain data security using LSB insertion steganographic method. In this approach, high security layers have been proposed to make it difficult to break through the encryption of the input data and confuse steganalysis too.

In 2008, a heuristic approach to hide huge amount of data using LSB steganography technique. In their method, they have first encoded the data and afterwards the encoded data is hidden behind a cover image by modifying the least significant bits of each pixel of the cover image. The resultant stego-image was distortion less. Also, they have given much emphasis on space complexity of the data hiding technique.

1.2 Security of text messages

This paper deals with the security of text messages at the time of sending it over the network. In our algorithm, we have used asymmetric key cryptography which means different keys are needed to encrypt and decrypt the data. Here we divide the domain of the key selection into different sub domains (a random prime number, a randomly generated number, decimal value of the pixel (only R) from the cover picture). In this approach we have given strength on division of the domain together with the key length. According to our concept, we encrypt the original text message letter by letter applying a function which involves certain mathematical operations using corresponding letters and also numbers from the original image. Then, we use two public keys and one private key for encryption and decryption. These keys are generated randomly following some constraints and equations. For encryption and decryption, we have used a mathematical operation called Multiplicative Modulo in between the text and the generated keys. The used mathematical relation is given below. (Say, a, b are any numbers and p be a prime number such that $0 < a, b < p$.). This technique constitutes the first layer of Security in our model.

2. New Methods

In the next attempt we have used one new method code_matrix mapping. In this method, the encrypted code is first is broken digit by digit. Next digits are converted into binary matrices having size DP (Depth of the cover Picture) X x where x gives the resultant code plus 1 where the code is obtained from the encryption procedure of the text. Here, the content of the matrices are not important and it can have any binary value. This approach incurs second layer of Security in our model.

After that we have used another new method matrix pix mapping. In this method the matrices obtained previously are mapped into zone of pixels having area DP X x (in bytes) C = remainder of (a*b)/p, where again x represents the same (previously mentioned) and DP represents the depth of the picture, by using Steganography (Least Significant Bit of the pixel bytes are modified). Here, also after mapping of each matrix we have left one pixel unchanged after mapping a certain set of matrices (constituting a word) we have left 2 pixels unchanged. This type of operation implements third layer of Security in our work. The change in Least Significant Bit in the value of Red-Green-Blue (pixel) is likely to be undetectable by human eye. Even if the hackers could predict that a message is hidden inside the image, then they could at most acquire the matrices.

These matrices should be effectively converted to obtain the encrypted data. After this, the encrypted data needs to be decrypted with the use of the private key to obtain a cipher code which has to be again decrypted to finally retrieve the original text. So, for the hackers it is very difficult to salvage the data crossing these Multiple Layers of Security.

3. SYSTEM ARCHITECTURE

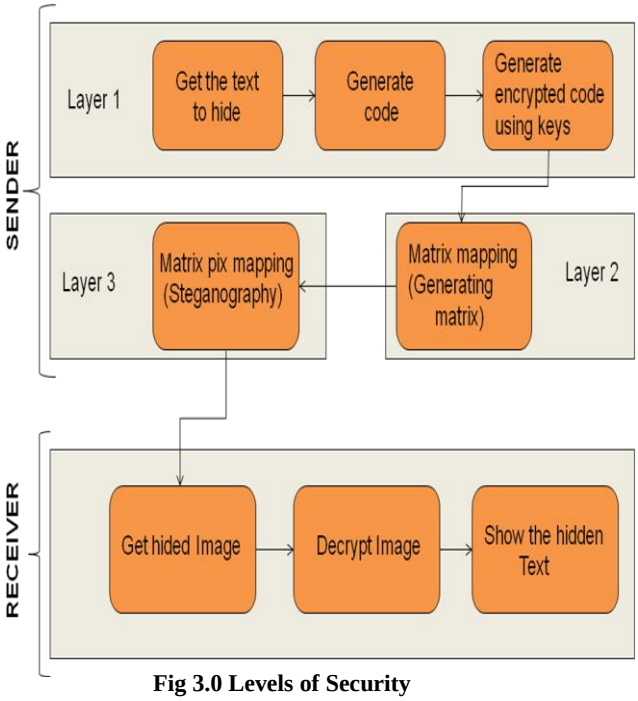

Fig 3.0 Levels of Security

In this system three layer of security has been implemented. In layer 1, the actual text message is converted into number code and two random public keys are generated. Using the keys the number code is encrypted. In layer 2, matrix is generated for each encrypted number. Finally in layer 3, the matrix obtained

is embedded into an image using steganography. The detailed information of each layer is explained below.

Layer 1

Layer 1 composed of number code conversion, public key generation and matrix generation. First the text that is to be sent are accepted. Then for the each character of the accepted text corresponding number code is generated. Here the number code system used is ASCII (American Standard Code for Information Interchange).
Once the number code is been generated, the next step is generating two public keys. Generate a prime number n, Where n > the highest number assigned to the alpha numeric character (if ASCII is used then n > 255), and n <= 9999. Randomly generate a number b, Such that b < n. Here b and n are the two public keys which are generated randomly. After generating the two keys, the number code is encrypted digit by digit and each digit is encrypted using the formula: c=(a*b) mod n.

Where

c - Encrypted number for the digit.
a - Number code for the digit.
b, n - Generated public keys.

Layer 2
In Layer 2, matrix is generated for each encrypted digit. Matrices are generated for the encrypted numbers by code_matrix mapping method. Matrices have their row size equal to the depth of the cover image (where the text is going to be hidden). Matrices have their column size equal to the encrypted digit number plus 1.

For example, the encrypted code is 5 means the matrix for 5+1=6 is generated. The matrix for 6 will consist of 6 columns and 3 rows. Likewise matrix is been generated for each and every encrypted digit.

Layer 3
Once the matrices are generated Apply matrix_pix mapping(MPM) in which the zone of pixels are selected whose area is DP (Depth of the Picture) number of columns of the matrix. Now on the Bytes within that zone, Steganography using LSB bit modification is applied. After each digit a pixel is kept unchanged and after each code
2 pixels are left unchanged for identification. Obtain the resultant stego-image as final image.

4. PHASES INVOLVED

The various phases associated are:

4.1 Number Code Generation

At first, the original message that is to be hidden is retrieved as input from the user.

- Then the message is broken digit b digit and converted to number system.
- The number system chosen here is ASCII code.

4.2 Key Generation

- The number code generated is encrypted by using keys.
- Here two public keys (b and n.) are generated for encryption.
- b and n are prime numbers such that (n>255 and n<=9999).
- After generating the two keys, the number code is encrypted digit by digit and each digit is encrypted using the formula: c=(a*b) mod n

4.3 Matrix Generation

- Matrices are generated for the encrypted numbers by Code Matrix Mapping method.
- Each digit of encrypted numbers is converted to a matrix.
- Matrices have their row size equal to the depth of the cover image (where the text is going to be hidden).
- Matrices have their column size equal to the encrypted digit number plus 1.

4.4 Code Matrix Mapping Algorithm

Input: Hidden Text
Output: Binary Matrix

Procedure:

- Convert the Individual Characters of the text to its corresponding ascii value.
- Each ascii value is encrypted using a mathematical function called Multiplicative modulo(Mm).
- Generate the Matrix for the encrypted values.

4.5 Matrix Pix Mapping Algorithm

- The Matrices obtained previously are mapped into zone of pixels.
- Mapping is done by using Steganography.

4.6 Embedding into Multimedia Object

- Matrix obtained is used to add with LSB (Least Significant Bit) of an object.
- Finally matrices generated will be hidden inside the cover object.
- Final object is sent to the receiver.

4.7 Decryption and Retrieval

- A random Private Key (d) is generated.
- "d" is generated using the formula: d*b = (1 + k*n), where k is any integer and d < n.
- Receiver decrypt the number using the private key d with the help of the formula: a = (c*d) mod n, where "a" is the encrypted number for the text.
- Convert the numbers to obtain the original text.

5. EXPERIMENT DETAILS

The proposed system has been experimented in Java and the results are as follows:

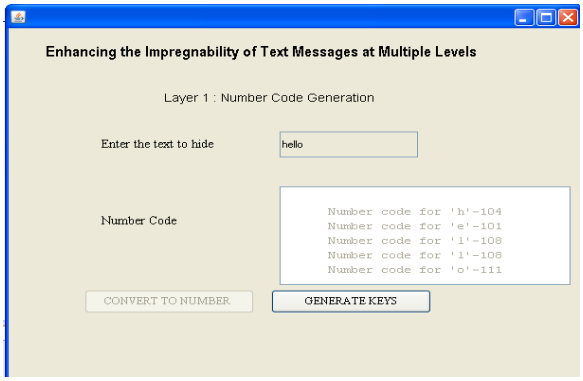

Fig 5.1 Number Code Generation

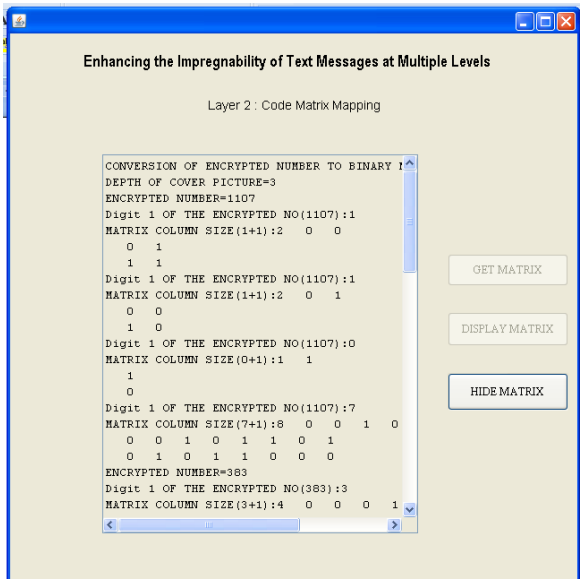

Fig 5.2 Matrix Generation

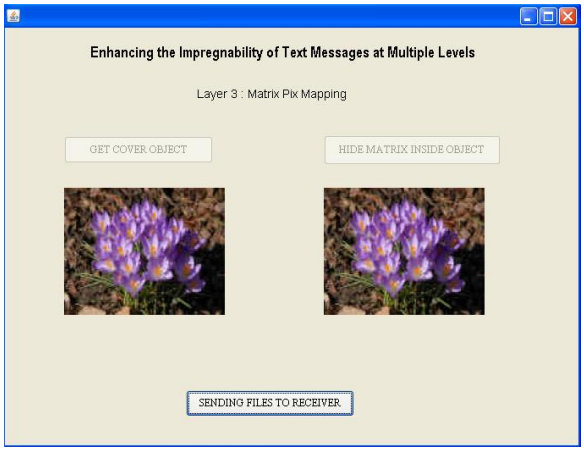

Fig 5.3 Matrix hidden successfully

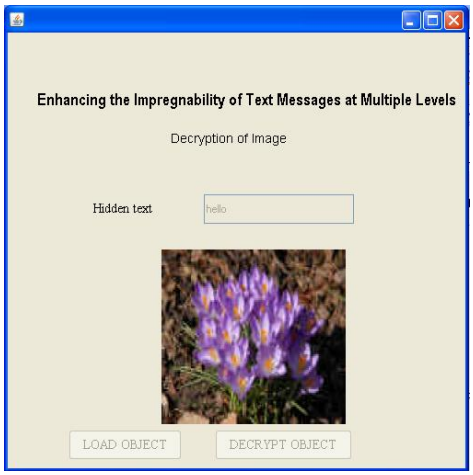

Fig 5.4 Decryption

6. CONCLUSION

The proposed approach has many applications in hiding and coding messages within standard media such as audio or videos. Also the model does not depend on the type of the text that is to be hidden. Any type of text can be used (even text of different language) and to work with it, the corresponding number system has to be chosen (here, the one used ASCII).

In future, the study of more steganalytic techniques for text messages will to extend the model to hide the encrypted message into an audio file and further enhancement on secure transfer of message through mobile communication.

7. REFERENCES

[1] "Text Steganography: A Novel Approach" Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay & Tai-hoon Kim International Journal of Advanced Science and Technology Vol. 3, February 2009.

[2] "A Tutorial Review on Steganography" IC3 – 2008.

[3] "Hiding Encrypted Message in the Features of Images", Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh IJCSNS, VOL. 7, No.4, April 2007.

[4] "Image based steganography using LSB insertion technique", Sutaone, M.S., Khandare, M.V IEEE WMMN pp. 146-151, January 2008.

[5] "A Multi Layer Security Model for Text Messages" Debnath Bhattacharyya, Poulami Das, Debashis Ganguly, Swarnendu Mukherjee 2009 IEEE International Advance Computing Conference (IACC 2009) March2009.