Combined Implementation of Robust Cryptosystem for Non-invertible Matrices based on Hill Cipher and Steganography

Bibhudendra Acharya, Himanshu Agrawal, Ankit Modi and Upendra Kumar Agrawal
Department of E & TC, NIT Raipur, Chhattisgarh-492010, India
Email: bacharya.etc@nitrr.ac.in, {himanshuagrawal1989, ankitmodi12, upeagrawal}@gmail.com

***Abstract*—In this paper, we have combined the Robust Cryptosystem for Non-invertible matrices based on Hill Cipher technique with steganography method in order to securely transmit text message. The steganography method used is LSB insertion technique. The encryption and steganography methods are used subsequently along with two randomization technique: one of XOR the encrypted text and another of randomized LSB insertion in any cover image. These two layers of shuffling of text at different stages of encryption and steganography provide two extra layers of security and make the system robust against cryptanalytic attacks.**

***Index Terms*—cryptography, steganography, plaintext, stego-object, cipher**

I. INTRODUCTION

In the current world that we live in, of rapid growing technology, the reliance on the Internet for our daily lively hood (Banking, shopping, entertainment, news) is growing like never before. Simultaneously crimes (Identity-theft, hacking, spyware) are also on the rise. Consequently, computer security is becoming more and more important. By "computer security", we often refer to addressing three important aspects of a computer-related system: confidentiality, integrity and availability. Encryption clearly addresses the need for confidentiality of data, both in storage and transmission [2, 3].

Cryptography is the technique for securing the secrecy of communication. Over the years many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Along with this, the corresponding cryptanalysis methods have also been developed in order to breach the security feature of respective encryption process. Thus, it is sometimes essential to keep the contents of a message secret as well as to keep the existence of the message secret. The technique used to implement is called steganography. It is the art and science of invisible communication. Now steganography is increasingly being used for transmission of digital data over internet [4, 9].

This paper is organized as follows. Section II presents the algorithm and advantages & disadvantages of the classical Hill Cipher. Section III describes the algorithm for the use of non-invertible key matrices, which is the modified Hill Cipher. Section IV describes relevant techniques implemented in this paper. Section V presents simulation results. Finally in Section VI concluding remarks are outlined.

In this paper, we have used modified Hill Cipher to encrypt and decrypt the text message. As simple matrix multiplication and matrix inversion is used, the technique exhibits high speed and high throughput. Such a technique has several advantages such as disguising letter frequencies of the plaintext and its simplicity in computation [6, 7, 8].

II. CLASSICAL HILL CIPHER ALGORITHM

In the classical Hill Cipher, the process of encryption and decryption uses a key matrix K consisting of some numbers such that its determinant is non-zero (i.e. the key matrix is invertible) and the determinant relatively prime to 26. If these conditions are satisfied then the process of encryption and decryption will work. This condition of invertible nature of the key matrix reduces the key space for the cipher significantly, thereby making the cipher vulnerable to brute force attack. The basic equations guiding the process of encryption and decryption are [1]:

$$C = P * K \bmod 26 \quad \text{for encryption and}$$

$$P = K^{-1} * C \bmod 26 \quad \text{for decryption}$$

Where, P is the plaintext in matrix form, K is the invertible key, C is the cipher-text and K^{-1} is modular arithmetic inverse of K.

III. ROBUST CRYPTOSYSTEM ALGORITHM FOR NON-INVERTIBLE MATRICES MATRICES BASED ON HILL CIPHER

Rushdi A. Hamamreh and Mousa Farajallah in their research paper "Design of a robust cryptosystem algorithm for non-invertible matrices based on Hill cipher" have proposed an efficient technique for safe transmission of cipher and key [10].

A. Encryption:

1- The plaintext characters are converted into numerical numbers.
2- Only if the resultant determinant of key matrix K is zero then identity matrix is added.
3- The column vector $C = K \times X$ is calculated.
4- Calculate $C1 = fix(C / P)$, $C_2 = \bmod(C, P)$.
5- The numerical numbers (C_1, C_2) is converted into characters.

DOI: 02 ACS.2010.01.167

B. Decryption:

1- The two sequence of cipher-text (C_1, C_2) is converted back into numerical numbers (Y_1, Y_2).
2- Only if the resultant determinant of key matrix K is zero then identity matrix is added.
3- The column vector $P = inv(K) \times ((Y_1 \times 256) + Y_2)$ is calculated.
4- The numerical numbers P is converted into characters.

IV. PROPOSED METHOD

The proposed method integrates the Robust Cryptosystem for Non-invertible matrices based on Hill Cipher technique with Steganography using LSB insertion. First of all we implement the modified Hill cipher resulting into encrypted text. XOR operation is performed with the encrypted text with a particular password/key sequence, known only to the sender and the receiver. This XOR has the property of completely permuting the encrypted sequence. The resultant output XOR-encrypted text is then converted into ASCII values which are hidden inside any cover image. This insertion of ASCII values inside the cover image takes place in a randomized manner guided by a numeric key. This key is actually a seed for a random number generator which produces a unique random number sequence for a particular value of seed. Thus, the randomized LSB insertion into the cover image takes place as per the random number sequence. The random number generator is shared by sender and the receiver. Thus, during transmission, we need to send only the key for modified Hill Cipher, XOR key and the seed for random number generator. Finally, these techniques applied subsequently one after another results into a stego-object which contains the encrypted text, recoverable by the receiver.
Proposed Algorithm

A. Sender Side:

i. Encryption

1. One time session key 'K' of dimension m×m for encryption is taken; if determinant of key matrix is zero then identity matrix is added to it to make it invertible.
2. The cipher text C is calculated by equation C=K*X; C is a matrix of the order m×n.
3. This ciphered text is broken into two parts by dividing each element of cipher matrix by 26 (to keep cipher text in form of alphabets only) these two parts are calculated by equations

C_1 = FLOOR(C/26), C_2 = MOD(C, 26).

C1 & C2 are of the order m×n. so number of elements gets doubled in comparison to original text.

ii. Xor Technique

Cipher text produced by Hill Cipher formed above is XORed bitwise with a password given by the user.

Now this matrix is broken into 2 parts by dividing it by 26; storing quotient in one matrix 'C1' and remainder in

iii. Steganography Hiding

1. Text is broken into one less than as many parts as there are blocks in cover image.
2. Depending on the seed (numerical key) given to the random sequence generator, a unique random number sequence is generated which determines the randomization of the bit hiding of text into the cover image.

B. Receiver Side:

i. *Steganography Unhiding*

1. We generate the random sequence using the same random generator and the seed as in sender's end and using this random sequence, we unhide the encrypted text form the stego-image.
2. Consequently, techniques of Ex-or and decryption technique is used to recover the text.
3. XOR TECHNIQUE
4. Cipher text is taken as input and then XOR operation performed with the password given by the user to get cipher text of modified Hill Cipher.

ii. Decryption

1. Cipher text produced in step 1 is broken into two parts and reshaped into two matrices of order m*n, same as C1 and C2.
2. These two matrices are converted back into numerical numbers Y1 and Y2 respectively, by subtracting a suitable number.
3. Same key matrix is taken; if the determinant of key matrix is zero then identity matrix is added so as to make it invertible.
4. The cipher text is calculated by equation C = ((Y1*26) +Y2).
5. Text is recovered by equation P = inv (K)*C.

V. RESULTS & DISCUSSION

Let us take the plain-text used for encryption be "NATIONAL". Firstly it is converted into its ASCII equivalent number i.e.

Plain = [78 65 84 73 79 78 65 76]

Length of text is '8' characters so 1 character 'A' is appended to make its length a multiple of 3 (reason for this is explained later). So array becomes

Plain = [78 65 84 73 79 78 65 76 **65**] (length = 9)

In the next step 65 is subtracted from Plain to bring it in a range of 0-26 (as English language has 26 characters). So we get Plain = [13 0 19 8 14 13 0 11 0].

Key '*K*' used for encryption is a 3×3 key matrix

K = [17 17 5; 21 18 21; 2 2 19]

Now the message array is converted into a 3 × 3 matrix. If key were to be a 4 × 4 matrix then we would have made the length of message a multiple of 4. Cipher text 'C' is calculated by equation:

*C = K * Plain* = [316 439 187; 672 693 198; 387 291 22]

DOI: 02 ACS.2010.01.167

other matrix 'C2'. 65 is added to both matrices and they are reshaped into linear matrices and concatenated to form a single array of length twice that of original message.

This numerical array is then converted into character again. So in this example we get C as

C = MZOQ[LHHAEWXXRFFQW (length = 18)

This is encrypted text by Hill cipher technique. Now we XOR the C with a password 'NITR@2010'. In this step each character of both C and password is converted into its 8 bit binary equivalent, and bitwise XOR is done with respect to length of encrypted text.

On the receiver side first encrypted text is taken out of stego-object using same password dependent block selection algorithm. Then with this cipher text XOR operation is performed with password used earlier i.e. 'NITR@2010'. Now what we have is Hill based cipher text of length twice that of original text. In next step we subtract 65 to bring it to range of 0-26.This array is broken into 2 parts and reshaped into two 3×3 matrices same as C1 and C2.

Cipher text C is calculated by equation C = (26*C1) +C2.

Key *K* is taken as *K* = [17 17 5; 21 18 21; 2 2 19]

Plain text *Plain* is calculated as $Plain = K^{-1} * C$. 65 is added to *Plain* take it to ASCII range

Plain = [78 65 84 73 79 78 65 76 65]

Now this is converted back into character to get "NATIONALA". As we have added the last A in order to adjust the length of the cipher text, it is deleted to get the original text back as "NATIONAL".

VI. CONCLUSIONS

Proposed technique for secure transmission of text has covered many limitations and insecurity of older techniques of similar kind. Moreover, there are many levels of security provided in our proposed algorithm including the XOR technique and randomized LSB rather than linear LSB steganography. Individual layers of protection and benefits are discussed below:

- The proposed technique is robust against known-plain text attack and it covers the problem of limited key space of classical Hill Cipher is covered, because of use of Cryptosystem for Non-invertible matrices.
- The randomized steganography with its unique seed for a particular random sequence makes the cryptosystem very strong. Even if the intruder finds out the unique seed, because this seed is not directly used for randomized steganography, such a revelation is useless. The intruder will need to find the random sequence which guides the process of randomized LSB insertion. As this random sequence is never transmitted via channel, rather generated at sender & receiver, the possibility of knowing this random sequence is ruled out.

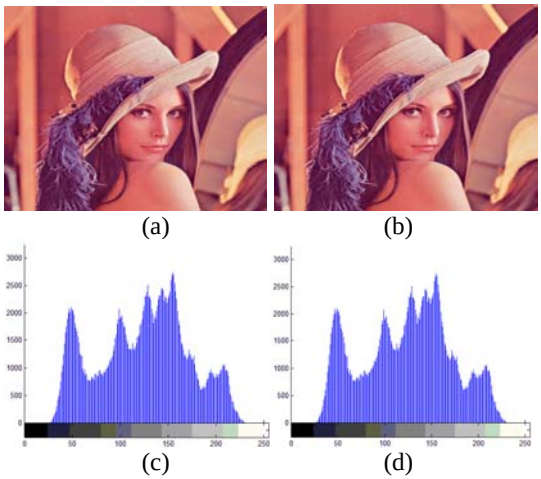

Figure 1. Cover Image (a), Stego Image (b), Corresponding Histograms (c & d).

- Above all this, we have used one-time session keys for the modified Hill Cipher encryption. Hence, the security in enhanced further.

Finally, the proposed algorithm involves only simple matrix multiplication, XOR operation and random sequence generation. Hence, it is very efficient in terms of consumption of time.

REFERENCES

[1] Lester S. Hill, Cryptography in an Algebraic Alphabet, *The American Mathematical Monthly*, Vol. 36, No. 6. (Jun. - Jul., 1929), pp. 306-312.

[2] G.R. Blakley, Twenty years of cryptography in the open literature, Security and Privacy 1999, Proceedings of the IEEE Symposium, 9-12 May 1999.

[3] W.-K. Chen, Scott Sutherland, "An Introduction of Cryptography", MSTP MATH WORKSHOP, 2005.

[4] Forouzan - Behrouz .A "Cryptography and Network Security", McGraw Hill. 2008.

[5] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall. 2006.

[6] Ismail, I.A., Amin, M., Diab, H., 2006. How to repair the Hill Cipher.*J. Zhejiang Univ*. Sci. A, 7(12):2022-2030.

[7] Jeffrey Overbey, William Traves, and Jerzy Wojdylo, "On the Keyspace of the Hill Cipher", Cryptologia, 29(1), January 2005, pp59-72.

[8] Adam J. Elbirt, Christof Paar "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography", IEEE Transactions on Parallel and Distributed Systems, May 2005.

[9] Cryptography and Network Security by William Stallings, Fourth Edition.

[10] Rushdi A. Hamamreh, Mousa Farajallah, "Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher", *International Journal of Computer Science and Network Security*, 2009; pp 11-16.

DOI: 02 ACS.2010.01.167