Secure Steganography Algorithm Based on Cellular Automata using Fibonacci Representation and Reverse Circle Cipher Application for Steganography

Nandan Makarand Deval

Abstract- Steganography is the act of hiding a message inside another message in such a way that can only be detected by its intended recipient .The process of hiding information inside another media is called steganography .In this technique the basic idea of steganography based on cellular automata using Fibonacci representation. The pixels color component is decompose into Fibonacci domain to extent more available bit-planes which can be used for data hiding for encryption we use reverse circle Cipher .This uses circular substitution and reversal transposition to exploit the benefits of both confusion and diffusion. With the help of these techniques we enhance the capacity of data hiding within image and security.

Keyword: Steganography, cellular automata, Fibonacci Representation, encryption, Cipher.

I. INTRODUCTION

Since the rapid development of network technique and recent advancement in cryptography brought a whole tub full of algorithm and techniques. In this network technique valuable data is transferred via internet. These techniques focus on fortifying the code making it more and more unbreakable. There have been many steganographic techniques which have been developed to protect information when it is transferred via internet. This technique can be categorized as spatial and frequency domain technique but only few of it focus on performance of the algorithm in terms of time and space complexity. This is because performance of the algorithm and the level of security has been a trade off. Hence it is only natural go for most alternative security.

II. PROPOSED METHOD

This proposed algorithm that hides secret bits into higher LSB layers of image pixel color component in a Fibonacci domain in order to improve the robustness and security of hidden data embedded into stego-image. The algorithm is as follows:

Step 1: The user enters string or message that is used for encryption. It encrypts and decrypts using reverse circle cipher algorithm and key stream generator maps status cell in grid into binary representation. Encryption decryption algorithm

Encryption

1. Start
2. Clear all buffers;
3. Open plane text input file
4. Open cipher text output file;
5. Obtain key;
6. While(!eof(plaintext))
7. {
8. Load p from plaintext file;
9. For(i=0;i<R;i++)
10. $C_i = f(P_i, k_{(0+len(k))^i})$
11. Reverse the content of c;
12. Append C to cipher text file;
13. Clear C and P;
14. }
15. Close all files;
16. End

Decryption

1. Start
2. Clear all buffer;
3. Open cipher text input file;
4. Open cipher output file;
5. Obtain key;
6. While(!eof(cipher text))
7. {
8. Load C from cipher text file;
9. Reverse the content of C
10. For(i=0;i<R;i++)
11. $P_i = f^{-1}(Ci, k_{(0+len(k))^i})$
12. Append P to plaintext file;
13. Clear C and P
14. }
15. Close all files;
16. End

Step 2: The secret message is encrypted by applying the bitwise XOR operator to every bit using a generated key stream.

Step 3: The selected color component is represented into Fibonacci representation

Step 4: The secret bits are embedded into kth LSB layer of decomposed image pixel color component. **Step 5:** The adaptive adjustment is applied to minimize the distortion of color component of image pixels. The blue color component of image pixel is used to embed the secret bit in order to further reduce the distortion of the cover-image. In general, the value of the image pixel is a combination of three color components (Red, Green, and Blue), thus, the blue color component modification causes less distortion than

Manuscript Received on January 2015.

Nandan Makarand Deval, Department of Computer Engineering, Marathwada Mitra Mandal's College of Engineering Pune, Maharashtra, India.

green and red . Therefore, the secret bits are embedded into green and blue color components identified by the value of the bit in a key stream in order to reduce the distortion of the stego-image and increase the security performance of hidden data. If the value of current bit in key stream is 0, the green color component is selected to embed secret bit and vice versa.

A. Fibonacci Decomposition

In a color image, a color component of a pixel can be represented in decimal value in range [0, 255]. The value of a color component in the binary system is equivalent to 8 bit representation as follows.

$$iiD\ b\ b\ b\ bi = + + + = \sum 2\ 2\ ...\ 2\ ,7022110\ 0\ 1 \quad (1)$$

where $b \in \{0, 1\}$.

For this reason, the decomposition of a pixel color component of an image is 8 bit-planes and this presentation does not introduce the redundant. Since the message bit is embedded into the LSB of color component, it is vulnerable even with a small change of the pixel. The message bits need to be embedded into a higher bit-planes with minimal distortion in order to increase the robustness of the LSB embedding scheme. The Fibonacci decomposition is very useful when it introduces 12 bit-planes to represent the values in Range [0, 255] [10].

B. An Adaptive Adjustment LSB Algorithm

The message bits are embedded into higher LSB layers in order to increase the robustness of hidden data against any common modification attack (such as Gaussian or Salt and Pepper noise). This process causes significant distortion to the cover-image pixel. From this fact, the adaptive adjustment is applied after embedding to reduce the distortion. The proposed algorithm, which hides message bit *b* into the k^{th} LSB layer of a Fibonacci representation of an image pixel color component, includes two steps as follows.

Input: decomposed color component with 12 bit-planes into Fibonacci representation $c = (c11, c10 \ldots c0)$.

Output: decomposed color component into Fibonacci representation with a secret bit embedded.

Step 1. Embedding the message bit *b* into the *k*th LSB layer of *c*

if (*c*k==0&&*b*==1) **{** // case 1
set *c*k = *b*;
set all the bits (*c*k-1, *c*k-2,…,*c*1) to 0
if (*c*k+1==1) **{**
set *c*k+1=0;
set all the bits (*c*k-2, *c*k-4,…,*c*2) to 1 in a such way that *c* will
contain no consecutive 1's.
}
}
else if (*c*k==1&&*b*==0) **{** // case 2
set *c*k=*b*;
set all the bits (*c*k-1, *c*k-2,…,*c*1) to 0
set all the bits (*c*k-1, *c*k-3,…*c*1) to 1 in a such way that *c* will
contain no consecutive 1's.
}

Step 2. Adjust if the value of color component larger than 255 after embedding.

if (*convfib2dec*(*c*)>255)**{** // case 3
find the first bit 1 on the right of *k* and then set to 0 if it
is found.
set all the bits (*c*k-1, *c*k-2,…,*c*1) to 0
set all the bits (*c*k-1, *c*k-3,…*c*1) to 1 in a such way that *c*
will contain no consecutive 1's.
}

where *convfib2dec(x)* is the user's function that convert Fibonacci representation x to decimal.

With the adaptive adjustment, the message bit $b = 1$ can be hidden into the LSB layer of cover pixel's color component, which a neighbor in the previous bit-plane is a value of 1. As a result, the proposed algorithm overcomes the limitation of the Zeckendorf's theorem. The image pixel color component is represented into Fibonacci domain. After that, the secret bit is selected from the kth LSB layer of decomposed image pixel color component.

System Architecture

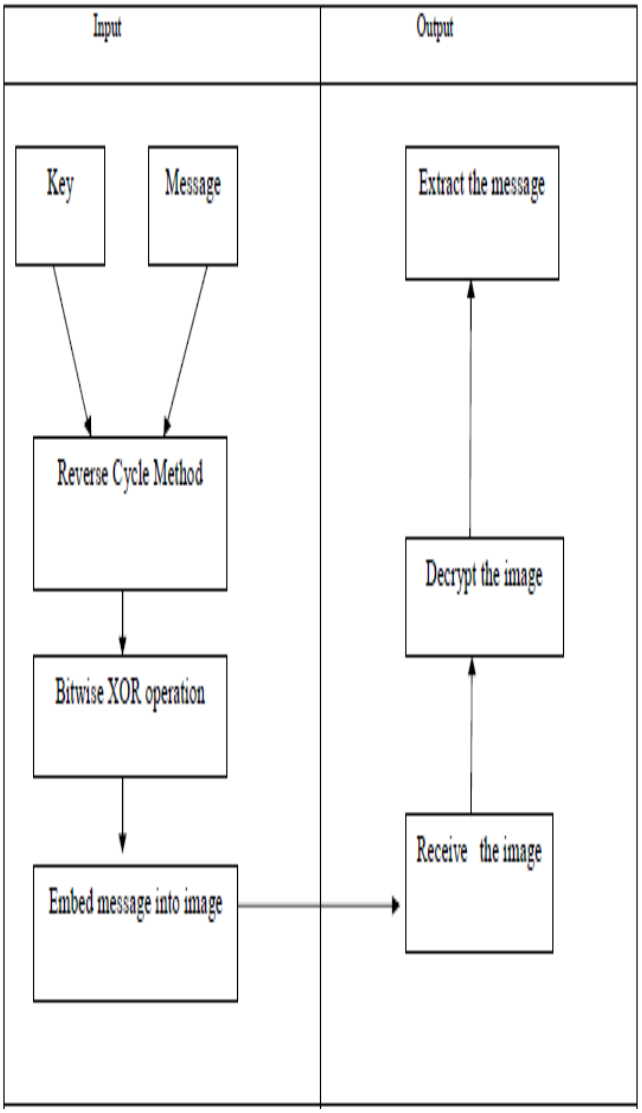

Fig. (1)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

System Graphical User Interface

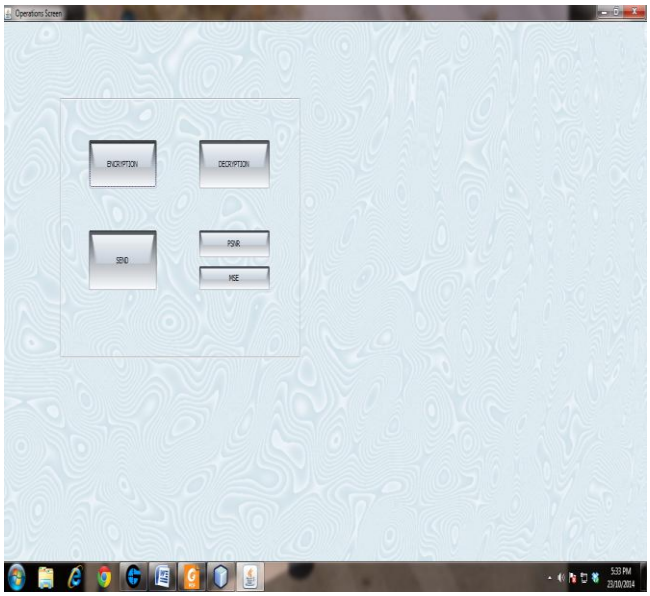

Fig. (2)

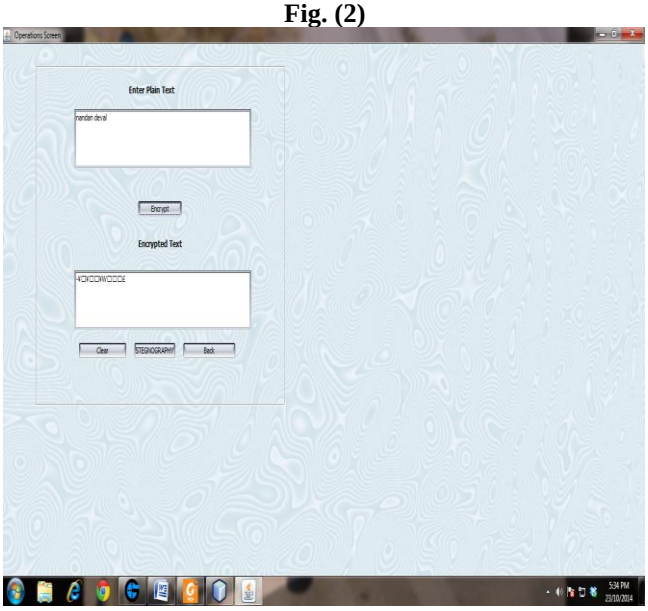

Fig. (3)

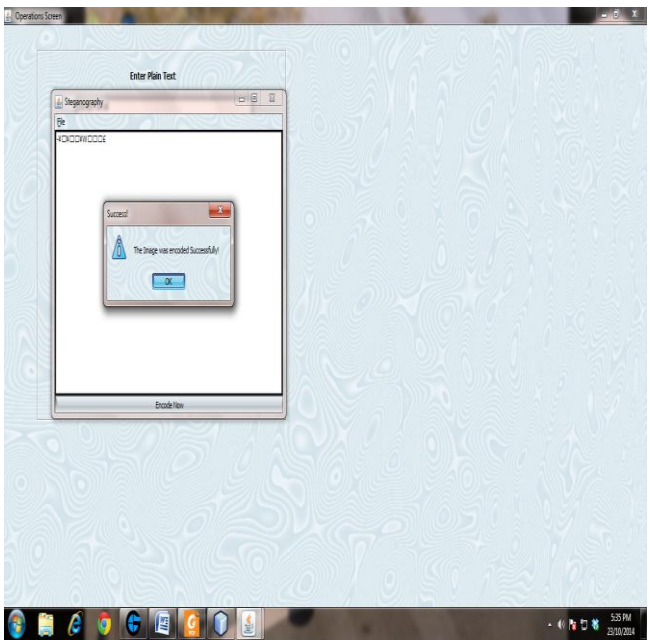

Fig. (4)

III. CONCLUSION

Successful design, development and deployment of java API that provides simple ,efficient reverse circle cipher cryptographic encryption and decryption and Fibonacci steganography to the user so that they can be used to secure communication in an application over internet i.e. you can send mail stego- image and can decrypt on another machine having this java API. This also proposes a secure adaptive steganography algorithm based on cellular automata and Fibonacci bit plane decomposition. The size of stego -image differs with original with not much of greater extent even if large amount of data is hidden. Fibonacci representation introduces more available bit planes which can be used in data hiding. The secret bit can be embedded d into higher LSB layers with low distortion on cover image. Further-more the system has been implemented with a view to keep the interface simple and consistent, the proposed algorithm enhances the performance of security of hidden data.

IV. FUTURE SCOPE

In further algorithms to come large amount of data can be hidden in the image. Reverse circle cipher encryption method can also be enhanced to make data unreadable and secure and use of private and public key in encryption process can be developed.

REFERENCES

1. J. Fridrich, M. Goljan, and R. Du, "Detection of LSB steganography in color and grayscale images," Magazine of IEEE Multimedia Special Issue on Security, pp. 22-28, October 2001.
2. S. Dumitrescu, X. Wu and Z. Wang, "Detection of LSB steganography via sample pair analysis", IEEE Transactions on Signal Processing, vol. 51, no. 7, pp. 1995-2007, July 2003.
3. A secure steganographic algorithm based on Cellular Automata using Fibonacci representation Tuan Duc Nguyen Department of Computer Science Faculty of Science, Khon Kaen University Khon Kaen, Thailand
   Somjit Arch-int Department of Computer ScienceFaculty of Science, Khon Kaen University Khon Kaen, Thailand june 2013
4. Bruce Schneier, "Applied Cryptography – Protocols, Algorithms, and Source Code in C", John Wiley and Sons Inc. Second Edition. pp. 12-30.
5. Matt Bishop, "Computer Security: Art and Science", Pearson Education, pp. 270-300, 2005. William Stallings, "Cryptography and Network Security: Principles and Practices" Fourth Edition, Pearson Education, pp. 30-150, April 2006.
6. Yee Wei Law, Jeroen Doumen, and Pieter Hartel. Survey and Benchmark of Block Ciphers for Wireless Sensor Networks. *Transactions on Sensor Networks (TOSN).* ACM February 2006
7. Reverse Circle Cipher for Personal and Network Security Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. VisumathiJeppiaar Engineering College Chennai, Tamil Nadu, India