Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Improving Classical Fibonacci in Steganography

Zainalabideen Abdual Samad Rasheed
Education College/ kufa University,
Iraq

Abstract— for many years, people have created different steganography techniques for hiding information. Steganography is a method of hiding information in such a way that even the recipient cannot guess the existence of the hidden information unless he is aware of the action of hiding message. The purpose of steganography is to allow a secure communication between two parties to exchange their secret message in a safe way. This achieves privacy and protects data from being altered. In this paper an improvement of classical Fibonacci has been made to solve the limitation of this method .the limitation of classical Fibonacci case by Zeckendrof theorem. This improvement leads to increase capacity of hiding by making all pixels values in cover file good candidates for hiding. And decrease time of steganography algorithm as well as not key requiring.

Keywords— Steganography, Cryptography, Classical Fibonacci, Zeckendorf's Theorem, Bit Plan.

I. Introduction

The idea of steganography is to use a cover object as a medium to transfer secret information securely. In other words information with different formats can be sent using different cover object formats. Such examples include hiding a text format in a video, image, or audio. Steganography is a Greek word consists of two segments 'stega' and' nography' ,the first segment means covered and the other means writing. Writing on wax-covered tablets was used in Ancient Greece. The histories of Herodotus was the first document that been used steganography, after Demeratus used wax-tablet cover for sending messages. Secret messages were written on tablets and covered with wax to hide messages. Later, Invisible ink was used in steganography by people. Security of information has one of the important issues of communication due to a huge use of internet. Different techniques have been created for securing the privacy of communication and for keeping the content of a data secret [1].Three types of different technologies of security systems are commonly used today; they are Cryptography, steganography and watermarking. For communication and authentication cryptography has been used, while both steganography and watermarking are used for hiding information. Cryptography is a method that encrypts data before communication where only the authorized side is able to decrypt the data after receiving it. However, steganography is a method to hide data in away such that no one can feel the existence of data. Recently, steganography has become widely used in the development of information security. Digital media can be used to hide secret information such as image, video, audio, text etc. [2] [3].

II. STEGANOGRAPHY

According to Cachin [4], it can be explained a steganography algorithm by looking at the secure communication between sender and receiver such that this communication will be secured from the wardens. Digital steganography is the science or art of hiding digital information in digital media so that no one other than the recipient can feel the real existence of this information in the given media. This science represents a form of security communication or secure transmission of information between participants in safe method. Steganography is considered to be a very effective method in securing information .In steganography the data type of information to hide and the cover object can be either of the same or different format .i.e. the cover object can be any format type like image, audio, video, text etc. and the data can be any type of format too [5] [6].Figure 1 below illustrates the basic idea of any steganography process.

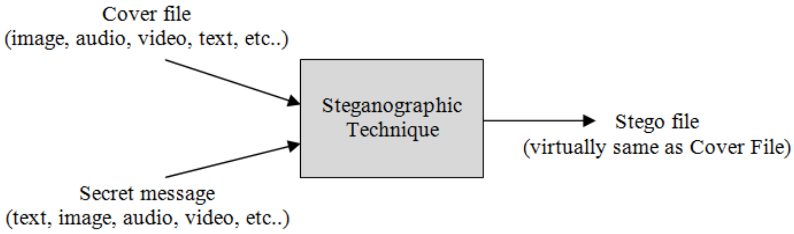

Figure 1: Fundamental scheme of steganography process [6]

In fact, there is a relation between the size of the secret message and the size of the cover file, such that making the size of the cover-file larger than the size of secret message will allow more flexibility to add and distribute the secret message within the cover-file [7].

III. BASIC FIBONACCI

"The classical Fibonacci numbers introduced in the 13th century by Leonardo of Pisa" .The sequence Fibonacci numbers is defined by the relation F (N) =F (N-1) +F (N-2). Where F (0) =1 and F (1) =1.Fibonacci sequence is [1,1,2,3,5,8,13,21,34,55,89,144,233,377,… etc.]. It can be used to represent any numeric value like binary representation. If N is the number of bits allocated to represent any numeric value then it will be easy to distinguish between binary representation and Fibonacci representation. For example if N =4 then the maximum numeric range is from [0...15] according to binary representation (1, 2, 4, 8) for four bits. Using Fibonacci representation the maximum numeric range is from [0...7] according to Fibonacci representation (1, 1, 2, 3). For example, if N =8 then the maximum numeric range is from [0...255] according to binary representation (1, 2, 4, 8, 16, 32, 64,128) for four bits. Using Fibonacci representation the maximum numeric range is from [0...51] according to Fibonacci representation (1, 1, 2, 3, 5, 8, 13, 21). However, in binary representation there is a unique code representation for each number either for the values in [0...15] or for the values in [0..255]. Using Fibonacci, code representation could be more than one for the same number. Example, the number 51 in binary system, is represented by the unique code 110011 i.e. (1+2+16+32), whiles in Fibonacci representation, it can be represented by (34+13+3+1) or (21+13+8+5+3+1).i.e. there are redundant codes when Fibonacci representation is used to represent the numbers. Using more than one code to represent the same number makes the decomposition process incorrect in the case of Fibonacci representation; however a unique code in binary representation makes the decomposition process always correct. Hence, for correct Fibonacci decomposition a unique code is needed. Zeckendorf produce a theorem to represent a Fibonacci unique code for positive integer numbers. "Each positive integer m can be represented as the sum of distinct numbers in the sequence of Fibonacci numbers using no two consecutive Fibonacci numbers." [8] [9] .

As a result from the previous presentation of Fibonacci sequence, this sequence can be used in steganography. It uses Fibonacci sequence to represent the pixel value instead of binary representation. I.e. 12 bits are used to represent the values from (0,255) instead of using 8 bits in binary system. The bit of secret message is written over the bit plan of the cover pixel .i.e. the secret message is converted to binary bit stream. The pixel value of the cover image which is selected for hiding the secret message is converted to Fibonacci representation, and then the bit plan of the pixel value of the cover image is replaced with the secret message. Finally, decompose the Fibonacci representation into the pixel value of the cover image. To retrieve the Stego image, the key of selected pixels are needed. The value of the selected pixel is converted to Fibonacci representation and secret message is reconstructed from the cross pounding bit plan [10] [11]. (Stego image mean the cover image which content the secret message. however, the bit plan mean a bit in cover image which is selected for embedding a bit of secret message)

IV. LIMITATION OF CLASSICAL FIBONACCI

The limitation is the condition of selected pixels. "The Zeckendorf condition is checked for each bit to be modified. If the condition is fulfilled, the bit is inserted otherwise the bit following it is considered" [10]. "Fibonacci LSB usually does not allow a fixed size embedding since not every pixel in the block is a "good candidate" for the embedding. To deal with Fibonacci redundancy, it is necessary to comply with Zeckendorf's theorem. If the selected pixel is not a "good candidate" (meaning that the current bit to be changed by 1 has a neighbour in the previous bit plan having also a value 1), then the next candidate pixel is selected" [9]. This condition means if the bit plan has ones as it neighbours either on left or right or both, it will not be used as a bit plan e. Actually Fibonacci steganography method suffers from this condition because it needs to select candidate pixel value that justify this condition, and also keeps track for which pixel is used for the retrieving process, as well as time to search and the limitation of capacity for embedding [12].

V. THE PROPOSAL

Our proposal is to set zeros for both neighbours of bits plan to justify the unique code (condition above) .i.e. two bits before and after a bit plan will be set to zeros if and only if the bit of secret message is 1. If the bit of secret message is zero it will not affect its neighbours. This solution allows using Fibonacci method without condition and to use all pixels value available in the cover image, as well as time to search will be decreased. Also in the retrieving process there will be no need to keep track of which pixel is used. However, setting zeros to both neighbours of bit plan in some cases could make the change to the pixel value higher than the traditional way but not very big because in Fibonacci sequence each number is coming from adding two previous numbers f(n)=f(n-1)+f(n-2). for example, if n=7 then the Fibonacci sequence is [21 13 8 5 3 2 1] and f(7)=f(6)+f(5)=13+8=21. In traditional way, if we want to use a 6^{th} bit plan for the embedding process the change to the value will be either to add or subtract 13 because the value of 6^{th} bit is 13.

However, in my method, setting ones to the 6^{th} bit and setting zeros to both neighbours 7^{th} and 5^{th} bit plan will result in (21+8)-13=16 and we can see that the difference of (13 and 16) is not so big. However, If a bit plan has one neighbour either right or left, then my method will still have less change than the traditional way. For example if the 7^{th} bit plan has only one neighbour, then setting zeros to this neighbour will result in (21-13)=8 and we can see that the difference of (13 and 8) is bigger than the previous. Also, if 5^{th} bit only has one neighbour then setting zero will result in (13-8) =5 while in traditional way is 13. Below is table 1 that shows all changes to the pixel value that could happen in embedding process for all bit plan in both methods; classical Fibonacci method and our proposal method. Moreover, the probability of finding both neighbours for each bit plan in Fibonacci is less than finding only one neighbour

TABLE 1 Changing the pixel value for all bit plans using classical Fibonacci and our proposal

11^{th}	10^{th}	9^{th}	8^{th}	7^{th}	6^{th}	5^{th}	4^{th}	3^{rd}	2^{nd}	1^{st}	**Bit plan s**

144	89	55	34	21	13	8	5	3	2	1	**Change to pixel value in classical way**
55	110	68	42	26	16	10	6	4	2	1	**Change to pixel value in our method if set zeros to both neighbour bit plan**
55	34	21	13	8	5	3	1	1	1	1	**Change to pixel value in our method if set zeros to right neighbour bit plan only**
144	55	34	21	13	8	5	3	2	1	1	**Change to pixel value in our method if set zeros to left neighbour bit plan only**

From table 1 we can see the probability of changing the pixel value in our method is less than the changing of the pixel value using the classical Fibonacci in most bit plan when a bit plan have neighbour ones.

VI. THE PROBABILITY OF EXISTING NEIGHBOURS TO THE BIT PLAN

As we mentioned in previous part, the changing in pixel value will be less if a bit plan has only one neighbour ones either in left or right. Below we will discuss the probability of existing two neighbours of ones to the all 12 bit plan s in Fibonacci sequence which is used to represent pixels value from [0...255].

Let n a level of bit plan in Fibonacci cod whose values should be from [1...12] for 12 bits Fibonacci representation. the Fibonacci value for each n will be : f(n)=f(n-1)+f(n-2) and the left neighbour for that bit plan is f(n+1) however ,the right neighbour is f(n-1) .Left neighbour value is f(n+1)= f (n) +f (n-1) .while the value after left neighbour is f(n+2)=f(n+1)+f(n).There are three probity for each bit plan for having ones neighbour: either has left neighbour, right neighbour or both. The percentage of each bit plan has only one neighbour is greater than both neighbours for representation pixel values from [0...255] as it clear from an example below:

If a bit plan n has two neighbour ones then the minimum value of this cod is [f (n+1) +f (n-1)] and maximum value of this code will be less than f (n+2).as shown from table 2 a 10^{th} bit plan in Fibonacci sequence whose value is (89) with left, right neighbours as well as the bit plan before and after.

A 10^{th} bit plan is f (n) =89

Left neighbour is f (n+1) =144

Right neighbour is f (n-1) =55

The minimum value is [f (n+1) +f (n-1)] = 144+55=199

The maximum value of this code will be less than f (n+2), I.e. maximum value < 233

I.e. the percentage of exist two of ones neighbour to the bit plan f (n) =89 in Fibonacci sequence will be appear just in pixels whose value from [200, 201,…232].as an example shows above if pixel value is greater than 232 will be have a new code for Fibonacci and the case of has two of ones neighbour will disappear.

TABLE 2 The 10^{th} bit plan in Fibonacci sequence f (n) with his neighbours

F(n+2)	**Left neighbour**	**Bit plan e**	**right neighbour**	**F(n-2)**
F(n+2)	F(n+1)	F(n)	F(n-1)	F(n-2)
233	144	89	55	34

It is clear from table 3 the probability of each bit plan for having two of ones for two neighbours(left and right) is less than the probability of having only one neighbour in Fibonacci sequence which is used to represent pixel value from [0..255].

TABLE 3

The probability of some bit plan for having two of ones neighbour for some bit plan in Fibonacci sequence

The probability of having two of ones for some bit plan in Fibonacci sequence	**Bit plan**
non	233
Non (because (233+89>255)out of range [0..255]	144
Just if pixel value From [200,201,…232]	89
From [123…143]	55
From [76….88]	34

VII. RESULT

The estimating parameters of the two stego covers have been performed using indigenous mat lab code in Intel Core3 Duo CPU processor @ 2.20 GHz, 6GB RAM. Our proposed methodology has been compared with classical Fibonacci and the results are tabulated in Table 4.the table shows PSNR and time of Stego_images(stego images.png) for all level of bit plans using two methods ,our proposed and classical fiboancci . morevere, aparctical proving have been applied for all types of image (jpeg,png and bmp) and gives the same result.

TABLE 4 PSNR and time of Stego_images.png using our proposal and classical fibonacci methods

Level of bit plan e	**PSNR of stego-image using our proposal**	**PSNR of stego-image using classical Fibonacci**	**time of our proposal Fibonacci**	**time of classical Fibonacci**

1st LSB	57.8803	57.4011	16.7278	19.0365
2nd LSB	57.0515	56.3189	16.8599	19.0365
3rd LSB	52.5144	51.6591	16.9743	19.0365
4th LSB	48.9379	46.5573	17.1423	19.5667
5th LSB	43.9569	42.4678	17.5976	19.8358
6th LSB	40.5302	38.1052	17.1744	19.0291
7th LSB	35.3940	33.7040	17.3849	19.0809
8th LSB	32.2058	29.7363	17.1065	19.9056
9th LSB	25.7393	24.8598	17.2408	19.7957
10th LSB	24.6463	22.5844	17.2838	19.9995
11th LSB	22.6243	21.4337	17.1591	19.4574
12th LSB	19.0034	19.0012	17.1590	19.4589

a) Time means the time of hiding and retrieving processes
b) Quality of stego image peak signal-to-noise ratio (PSNR)'' It is the measure of quality of the image by comparing the cover image with the stego image, i.e., it measures the statistical difference between the cover and stego image, '' [13].

The formula of PSNR is given by:

$$PSNR(dB) = 10 * \log(\frac{255^2}{MSE})$$

The formula of MSE is given by:

$$MSE = \frac{1}{mn} \sum_{0}^{m-1} \sum_{0}^{n-1} \|f(i,j) - g(i,j)\|^2$$

Where:
f (i ,j): is pixel value of cover image .
g(i,j): is the pixel value of Stego image.
mn: is the size of an image. [13]

VIII. CONCLUSION

It is clear from table 4, the quality of Stego_image (PSNR)of our proposal is better than classical fibonacci method because of the how zeros are set to the neighbouring bits of bit plan as mentioned in our propsal part. This results in less change to the pixel value hence high quality than the classical fibonacci . Relating to time, table 4 is shown that our method is better than the classical fibonacci because the time to search for a candidate pixel in classical fibonacci is longer than the time of search in our method. Also, the size of cover image which is needed for embedding process using classical fibonacci is bigger than the size of cover image using our proposal because not all pixels can be used for embedding process.morever,our propsal is not need to keep trak for which pixel has been used in hiding process to be use in retriving process.i,e our proposal more convenent than classical fibonacci.

REFERNCES

[1] Morkel, T., Eloff, J., & Olivier, M. (2005). An overview of image steganography.
[2] Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, *47*(10), 76-82..
[3] Silman, J. (2001). Steganography and steganalysis: an overview. *SANS Institute*.
[4] Cachin, C. (2005). Digital steganography. *Encyclopedia of Cryptography and Security*, 129-168.
[5] Natanj, S., & Taghizadeh, S. (2011). Current Steganography Approaches: A survey.
[6] Al-Othmani, A., Manaf, A., & Zeki, A. (2012). A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation.
[7] Verner E. Jr. Hoggatt, "Fibonacci and Lucas Numbers," *The Fibonacci Association*, Santa Clara, California, USA, 1972.
[8] Jr, V. H., Cox, N., & Bicknell, M. (1973). A Primer for the Fibonacci Numbers: Part XII. *The Fib. Quart*, *11*, 317-331.
[9] Picione, D., Battisti, F., Carli, M., Astola, J., & Egiazarian, K. (2006). A Fibonacci LSB data hiding tecnique
[10] Borgohain, R. (2012). Data Hiding Techniques using number decompositions. *Arxiv preprint arXiv:1206.4155*.
[11] Aroukatos, Nikolaos, et al. "Data hiding techniques in steganography using fibonacci and catalan numbers." *Information Technology: New Generations (ITNG), 2012 Ninth International Conference on*. IEEE, 2012. (in expalain of steganography)

[12] Nguyen, Tuan Duc, and Somjit Arch-int. "A Secure Stenographic Algorithm Based on Cellular Automata Using Fibonacci Representation." *Information Science and Applications (ICISA), 2013 International Conference on*. IEEE, 2013. (in limitation)

[13] Kumar, K., Raja, K., Chhotaray, R., & Pattanaik, S. (2010). Bit Length Replacement Steganography based on DCT Coefficients. *International Journal of Engineering Science and Technology, 2*(8), 3561-3570.

Zainalabideen Abdullasamd Rasheed University of kufa, Education of College, Najaf /Iraq Has a BSc (Baghdad University, Iraq), and MSc (Buckingham university, United).he has a long experience in teaching various computing practical courses at Baghdad university .at AL Kufa university, Mr. Rasheed teaches different courses like computer organization, operating system and computer architecture .he supervises undergraduate projects. He interest in data security (steganography and cryptography) and digital image processing (biomedical image and edge detection, de-noising images).E-mail: zain9999@live.com, Tel: 009647711131246 .Iraq.