Paper from Proceeding of the National Conference "Science in Media 2012" Organized by YMCA University of Science and Technology, Faridabad, Haryana (India) December 3rd -4th 2012 Published by IJMRS's International Journal of Engineering Sciences, ISSN (Online): 2277-9698
www.ijmrs.com

A study on time complexity of least significant bit steganography

Surbhi Singhania, Shailender Gupta and Bharat Bhushan, YMCA University of Science and Technology, Faridabad

***Abstract*—Steganography is the art of concealing private or sensitive information within a carrier for all intents and purposes, appears innocuous. It increases the level of privacy and security by making the confidential communication invisible. The most popular technique used is Least Significant Bit (LSB) substitution steganography. In this method, the least significant bits of pixels of cover image are replaced by secret data bits. This paper is an effort to find the impact of varying the number of least significant substitution bits of pixels by designing a simulator in MATLAB-11. The results show that as the number of LSB bits embedded is increased, the time complexity and capacity to embed secret data increases.**

***Index Terms*— Confidentiality, LSB, Time Complexity**

I. INTRODUCTION

With the recent advances in Internet computing and its invasion in our day to day life, the need for confidential and personal communication has increased. Privacy in digital communication is desired when confidential information is being shared between two entities via the computer communication. Existing technologies like cryptography [1-2] offer a solution by scrambling the confidential information in such a way that it cannot be read by anyone else except the intended recipient. However the issue with encryption is that the significance of the communication is highlighted because cryptographic data lacks the required logical sense [3] and can be easily recognized. Such illegible data can attract undue attention from eavesdropper, which is a threat for private and confidential communication. Thus privacy and confidentially is lost by the nature of cryptographic solutions. This has caused concerns for those people who desire private and confidential communication. In an attempt to address above security issue, information hiding techniques like steganography have shows some promising solutions. Steganography communication is difficult to trace and hence it makes the job of the hacker difficult because the hacker now has to track all network communication rather than just encrypted communication. This steganography feature increases the level of privacy and security by making the confidential communication invisible.

One of the simplest and oldest steganography techniques is least significant bit substitution [4-8]. This technique involves replacing the least significant bit of a first few pixels of the image with that of the bits of the data. In this paper we try to find the impact of varying the number of substitution bits on time complexity, capacity of the image to embed the data and image quality by designing a simulator in MATLAB-11.

The rest of the paper is organized as follows: Section 2 provides the algorithm of LSB. Section 3 gives the simulation set up parameters and the metrics used. Section 4 provides the results followed by conclusion and references.

Least Significant Bit (LSB) Steganography algorithm

Before discussing the algorithm we present some terminology used in the LSB algorithm.

- j is index of pixel of cover image
- ci is cover image pixel on to which secret text data is embedded.
- si is stego image pixel
- m is number of bits in message pixel

Algorithm 1:Embeding process of LSB Substitution

---

for $i = 1 \ldots\ldots\ldots, l(c)$ ***do***
$s_i \leftarrow c_i$
end for

for $i = 1\ldots\ldots\ldots$, *to* $l(m)$ ***do***
compute index j_i *where to store ith image bit*
$sj_i \leftarrow cj_i \leftrightarrow m_i$
end for

Algorithm 2:Extraction process of LSB Substitution

---

for $i = 1 \ldots\ldots\ldots, l(m)$ ***do***
compute index j_i *where to store ith image bit is stored*
$m_i \leftarrow LSB(cj_i)$
end for

The embedding process consists of choosing the subset {j1 to jm} of cover elements and performing the substitution operations c(ji) = mi on them which changes the LSB of the cji by mi(mi can be either 0 or 1). One could also imagine substitution process which changes more than one bit of the cover i.e. by changing two or more message bits in the least significant bits of the cover image which is done in our case.

In the extraction the LSB [9-10] of the selected cover elements are extracted and are lined up to reconstruct the secret message.

Simulation Set up :

a) Simulation Set up parameters

Table1: Set up parameters

Set Up parameters	
Processor	2.4 Ghz, i3 2370 M CPU
RAM	4 Gb
Operating system	64 bit
Number of bits substituted	1-4 bit
Tool used	MATLAB
Image type	TIF
Cover image size	512 X 619 pixels

b) Metrics Used

To measure the efficacy of the steganography algorithms, time complexity and capacity to embed secret data are used and defined as follows:

i. Time Complexity: Defined as the total time taken by processor to complete the embedding and extraction process.

ii. Capacity: The number of bits which can be embedded into the cover image. It should be clear that as the number of embedding bits increases the image quality deteriorates significantly.

Results

a) Impact on time complexity

Fig. 1 shows the time complexity when the number of embedding bits are varied. The following inference can be drawn:

- As the number of embedding bits in the cover image increases, the time complexity increases significantly since the capacity to embed data increases.
- The image qualities deteriorates slightly as the number of embedding bits increases

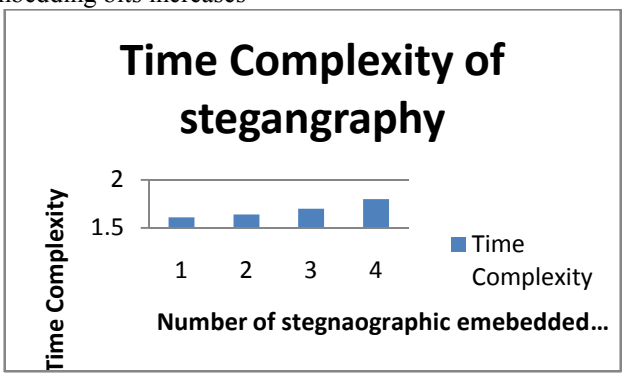

Fig 1 : Time complexity of Steganography

Fig 2 : Original image

Fig 3 : Result of applying 1 bit substitution

Fig 4 : Result of applying 2 bits substitution

Fig 5 : Result of applying 3 bits substitution

Fig 6 : Result of applying 4 bits substitution

b) Impact on capacity

Fig. 7 shows the impact on capacity by varying the number of embedding bits. We observe that the capacity doubles when the number of embedding bits is varied from one to two.

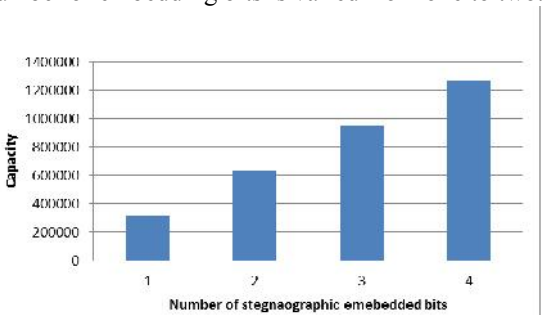

Fig 2: Capacity of the image to embed data for steganography process

1. Conclusion

The LSB modification technique provides an easy way to embed information in images. From the above results the following inferences can be drawn:

- The time complexity increases as the number of bits to be embedded in the cover image increases
- It may not be easily detectable by hackers when the number of bits embedded is increased up to four.
- The capacity increases as the number of bits to be embedded in picture increases.

These results can be very fruitful to researchers working in the direction of image processing and steganography

References

1. "Cryptography and Network Security: principles and practices", William Stallings, pearsons education, first Indian reprint 2003.
2. Neil F. Johnson and Sushil Jajodia, "Steganalysis of Image Created Using Current Steganography Software", Workshop of Information Hiding Proceedings, Portland Oregon, USA,15-17 April,1998. Lecture Notes in Computer Science, Vol.1525, Springer-Verlag (1998).
3. Sujay Narayana and Gaurav Prasad, "TWO NEW APPROACHES FOR SECURED IMAGE STEGANOGRAPHY USING CRYPTOGRAPHIC TECHNIQUES AND TYPE CONVERSIONS", in Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010.
4. Clair, Bryan, "Steganography: How to Send a Secret Message", 8 Nov. 2001 www.strangehorizons.com/2001/20011008/steganography.shtml.
5. Bender, W., D. Gruhl, and N. Morimoto, "Techniques for data hiding", IBM Systems Journal , vol. 35, no. 3/4, 1996, pp. 131-336.
6. Moller. S.A., Pitzmann, and I. Stirand, "Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best", in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 7-21.
7. Gruhl, D., A. Lu, and W. Bender, "Echo Hiding in Information Hiding", First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 295-316.
8. Kurak, C., and J. McHughes, "A Cautionary Note On Image Downgrading", in IEEE Computer Security Applications Conference 1992, Proceedings, IEEE Press, 1992, pp. 153-159.
9. Van Schyndel, R. G., A. Tirkel, and C. F. Osborne, "A Digital Watermark", in Proceedings of the IEEE International Conference on Image Processing, vol. 2, 1994, pp. 86-90.
10. Shailender Gupta,Ankur Goyal and Bharat Bhushan, Information Hiding Using Least Significant Bit Steganography and Cryptography" ,I.J.Modern Education and Computer Science, 2012, 6, 27-34.