Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Comparative Analysis of Two Approaches in Steganography

Sanchit Gaur[1], Rajiv Munjal[2]
Student MTech (cse), C.B.S Group of Institution, jhajjar, Haryana, India [1]
Assist. Professor (CSE Dept.), C.B.S Group of Institution, fatehpuri, jhajjar, Haryana, India [2]

Abstract: Steganography means hiding a message. Information hiding technique is a new kind of secret communication technology. Information hiding system uses multimedia objects like audio, images and text. Digital audio, images, text are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. Today the growth in the information technology, especially in computer networks such as internet, mobile communication and digital multimedia applications such as Animation, Video, and Audio etc.

Keywords: If C, LSB

I. INTRODUCTION

With the recent advances in computing technology and its intrusion in our day to day life, the need for private and personal communication has increased. Privacy in digital communication is desired when confidential information is being shared between two entities using computer communication. To provide secrecy in communication we use various techniques. One such technique is Steganography [1-2] that is the art of hiding the fact that communication is taking place, by hiding information in other information. Classification of stenography techniques based on the cover modifications applied in the embedding process is as follows:

A. Least significant bit (LSB) method

This approach [3-8] is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message.

B. Transform domain techniques

This approach embeds secret information in the frequency domain of the signal. Transform domain methods hide messages in significant areas of the cover image which make them more robust to attacks such as: compression, cropping, and some image processing, compared to LSB approach.

C. Statistical methods

This approach encodes information by changing several statistical properties of a cover and uses a hypothesis testing in the extraction process. The above process is achieved by modifying the cover in such a way that some statistical characteristics change significantly i.e. if "1" is transmitted then cover is changed otherwise it is left as such.

D. Distortion techniques

In this technique the knowledge of original cover in the decoding process is essential at the receiver side. Receiver measures the differences with the original cover in order to reconstruct the sequence of modification applied by sender.

II. APPROACH 1

The method to embed and extract the hidden message is described as follows.
First, we convert original message into cipher text with RSA algorithm.
Second, we convert cipher text into binary numbers.

- **Encoder**

1) Select the frames from Animation

a) Converting frames from animation for hiding message and decoy randomly.
b) RGB frames will be dividing into Pixels for hi.

2) Apply Embedding Algorithm[1]

If C is the value of the bit to be hide and Va is Least Significant bit in the Pixel.
Suppose we have 3 pixels in RGB format

	R	G	B
1st Pixel	(00101101	00011100	11011100)
2nd Pixel	(10100110	11000100	00001100)

3rd Pixel (11010010 10101101 01100011)

When the letter A, which binary representation is **01000001** is embedded into the least significant bits of this part of the frame, the resulting grid is as follows:

	R	G	B
1st Pixel	(00101100	00011101	11011100)
2nd Pixel	(10100110	11000100	00001100)
3rd Pixel	(11010010	10101101	01100011)

Apply the embedding algorithm we produce an efficient result.

- **Decoder**

1) Select the right frames for message extraction.

a) Select the frames from animation in which message hidden already.

2) *Extract the embedding bit by embedding mark.*

	R	G	B
1st Pixel	(00101100	00011101	11011100)
2nd Pixel	(10100110	11000100	00001100)
3rd Pixel	(11010010	10101101	01100011)

Where, we extract least significant bits of all pixels

APPROACH 2

- **Encoder**

1) Select the frames from video

a) Converting frames from video for hiding message and decoy randomly.

b) RGB frames will be converting into YCbCr format then choose Y (luminance) for message hiding.

c) We hide message in frequency of Y part of YCbCr.

d) We hide decoye in frequency of Y part of YCbCr.

2) Apply Embedding Algorithm

If C is the value of the bit to be hide and Va is embedded point in the frames. When C is 0, the Va is modified as:

$$\begin{cases} Va & \text{if } Va\%2 = 0 \\ Va + 1 & \text{if } Va\%2 = 1 \end{cases}$$

When C is 1, the Va modified as:

$$\begin{cases} Va & \text{if } Va\%2 = 1 \\ Va + 1 & \text{if } Va\%2 = 0 \end{cases}$$

Apply the embedding algorithm we produce an efficient result.

- **Decoder**

1) Select the right frames for message extraction.

a) Select the frames from video in which message hidden already.

2) Extract the embedding bit by embedding mark.

Where, Va is the embedded point and C is the embedded bits.

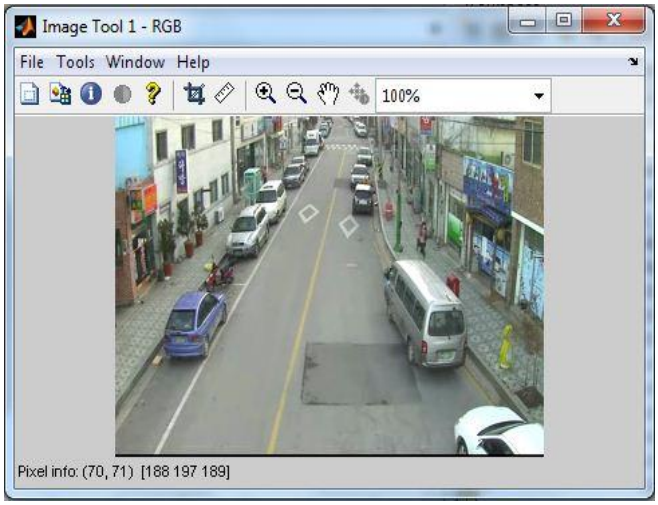
$$\begin{cases} C=1 & \text{if } Va\%2 = 1 \\ C=0 & \text{if } Va\%2 = 0 \end{cases}$$

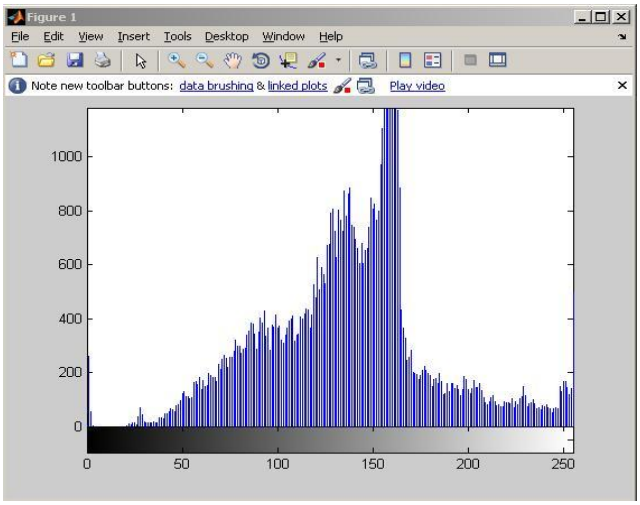
Where, Va is the embedded point and C is the embedded bits.

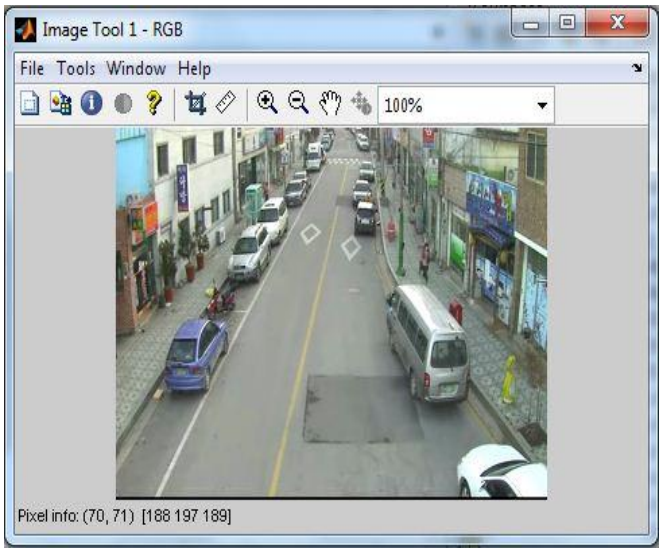
III. COMPARATIVE ANALYSIS

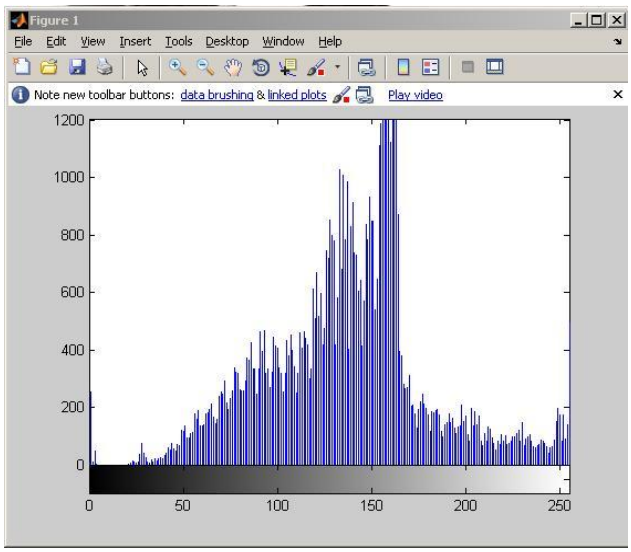
Figure 2 the 17th frame of animation rofl.to30second

Figure 3 the 17th frame of animation before hide 96 bit message rofl.to30second after hide 96 bit message









IV. CONCLUSION

This paper describes a technique to successfully embed data in an 8-bit color image. Additional features that could be added to this project include support for file types other than bitmap, and implementation of other steganographic methods. However, this research work and software package provides a good starting point for anyone interested in learning about steganography.

REFERENCE

[1] Chandra Prakash Shukla, Awadhesh Kumar Singh, "Secure Communication with the help of Encryption in Video Steganography", ISSN: 2279-0535. Volume: 3, Issue: 6 (Oct.- Nov. 2014).

[2] V.Sathyal, K.Balasuhramaniyam, N.Murali, M.Rajakumaran, Vigneswari, "DATA HIDING IN AUDIO SIGNAL, VIDEO SIGNAL, TEXT AND JPEG IMAGES", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.

[3] S. Suma Christal Mary, "IMPROVED PROTECTION IN VIDEO STEGANOGRAPHY USED COMPRESSED VIDEO BITSTREAMS", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766.

[4] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", ***I.J.Modern Education and Computer Science*, 2012, 6, 27-34** Published Online June 2012 in MECS (http://www.mecspress.org/)DOI:10.5815/ijmecs.2012.06.04.

[5] W. Bender,D. Gruhl,N. Morimoto,A. Lu,"**Techniques for data Hiding",** IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996.

[6] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, "Application of LSB Based Steganographic Technique for 8-bit Color Images", World Academy of Science, Engineering and Technology 50 2009.

[7] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis",Journal of Information Hiding and Multimedia Signal Processing c 2011 ISSN 2073-4212 Ubiquitous International Volume 2, Number 2, April 2011.

[8] Pratap Chandra Mandal, "Modern Steganographic technique: A Survey", International Journal of Computer Science & Engineering Technology (IJCSET).

[9] A. Swathi, Dr. S.A.K Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5.

[10] Dr. ATEF JAWAD AL-NAJJAR, "The Decoy: Multi-Level Digital Multimedia Steganography Model", 12th WSEAS International Conference on COMMUNICATIONS, Heraklion, Greece, July 23-25, 2008.

[11] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[12] Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk , Borko Furht, "New approaches to encryption and steganography for digital videos", © Springer-Verlag 2007.

[13] R. Balaji, G. Naveen, "Secure Data Transmission Using Video Steganography",

[14] Yam bern Jina Chanu, Themrichon Tuithung, Kh. Manglem Singh, "A Short Survey on Image Steganography and Steganalysis Techniques", IEEE-International Conference 978-1-4577-0748-3/12/$26.00 © 2012 IEEE.

[15] Salomon,D. , "Data Hiding in Text", - Springer,2003.

[16] Harish Kumar, Anuradha, "Enhanced LSB technique for Audio Steganography", IEEE-20180.

