ISSN No. 0976-5697

Volume 3, No. 4, July- August 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Encrypted Message Transmission Using Video File

Manoj T H*
M.Phil Scholar, School of IT & Science
Dr. G R D College of Science
Coimbatore, Tamilnadu, India
Manoj.kudur@gmail.com

A Santha Rubia
Assistant Professor, School of IT & Science
Dr. G R D College of Science
Coimbatore, Tamilnadu, India
Santharubia.a@grd.edu.in

Abstract: Steganography is the technique of hiding confidential information within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. This paper focuses on the strength of combining cryptography and steganography methods to enhance the security. The proposed method describes a novel method to transmission of encrypted message as Stegano image using video file.

Keywords: Image Steganography, Least Significant Bit (LSB), Cryptography, Cover Art, Caesar Cipher, Cipher Text, Stegano Image.

I. INTRODUCTION

Steganography is the art and science of hiding communication [1]; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography.

Information hiding generally relates to both watermarking and steganography [2]. A watermarking system's primary goal is to achieve a high level of robustness—that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile.

Steganography and cryptography are cousins in the spy craft family [3]. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not.

Digital signatures allow authorship of a document to be asserted. The signature can be removed easily but any changes made will invalidate the signature, therefore integrity is maintained. Steganography provides a means of secret communication which cannot be removed without significantly altering the data in which it is embedded. The embedded data will be confidential unless an attacker can find a way to detect it.

II. HISTROY

Throughout history, people have hidden information by a different methods and variations. For example, ancient Greeks wrote text on wax-covered tablets. To pass a hidden message, a person would scrape wax off a tablet, write a message on the underlying wood and again cover the tablet with wax to make it appear blank and unused. Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger's head. After the hair grew back, the message would be undetected until the head was shaved again. Invisible inks offered a common form of invisible writing.

With every discovery of a message hidden with an existing application, a new steganographic application is being devised. Old methods are given new twists. While drawings have often been used to conceal or reveal information, computer technology has, in fact, sparked a new revolution in such methods for hiding.

A. Modern Techniques of Steganography:

The common modern technique of steganography exploits the property of the media itself to convey a message.

The following media are the candidate for digitally embedding message [4]: -

Plaintext
Image
Audio and Video

B. Plain Text Steganography:

In this technique the message is hidden within a plain text file using different schemes like use of selected characters, extra white spaces of the cover text.

C. Image Steganography:

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS) or Visual Perception. HVS cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum. A picture can be represented by a collection of color pixels. The individual pixels can be represented by their optical characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s.

D. Audio/Video Steganography:

In Audio/Video steganography, secret message is embedded into digitized audio/video signal which result slight altering of binary sequence of the corresponding audio/video file. For video, a combination of sound and image techniques can be used. This is due to the fact that video generally has separate inner files for the video (consisting of many images) and the sound. So techniques can be applied in both areas to hide data. Due to the size of video files, the scope for adding lots of data is much greater and therefore the chances of hidden data being detected is quite low

III. OUR PROPOSED METHOD

This paper proposes a new algorithm to hide the data inside images using steganography technique. An algorithm is designed to hide all the data inputted within the image to protect the privacy of the data. Once the algorithm is adapted, user can send the stego image to other computer user so that the receiver is able to retrieve and read the data which is hidden in the stego image by using the same proposed system. Thus, the data can be protected without revealing the contents to other people.

Steganography Imaging System (SIS) is a system that is capable of hiding the data inside the image. The fields: image processing, software engineering. The system is using 3 layers of security in order to maintain data privacy. Data security is the practice of keeping data protected from corruption and unauthorized access.

A. Encryption at Sender Side:

Hiding image involves embedding the message in to the digital image. To embed the message, we consider gray scale Image, and these values often range from 0-255. In order to hide the message and data is first converted into byte format and stored in a byte array. The message is encrypted using Ceaser cipher. The Encrypted text is converted to Base 64. The binary value of encrypted text is embedded into image using LSB method [5]. The LSB of each 8bit byte has been co-opted to hide a text message. It uses the first pixel (at spot 0) to hide the length of message (number of character).

Algorithm
Input: Message M, to be hiding
Output: Encrypted Message
Method:

a) Get ASCII Value of Each Letter in a message
b) Use Caesar Cipher to Encrypt
c) Convert to Base 64.
d) Convert to Binary value
e) To get Stegano Image, Binary value is appended to Image using LSB method.
f) Stegano Image is added as Cover Art of the Video file.
g) Append Key in video File
h) Send the Encrypted video File.

B. Message Embedding in Digital Image:

Consider a Message "DEATH"
ASCII Value of Message is
DEATH = 68 69 65 84 72
Use Caesar Cipher to encrypt i.e., add 4 to all the decimal value.
72 73 69 88 76
Convert the encrypted message to base 64.
Encrypted value is SElFVFM==
Obtain the decimal value of encrypted message and convert to Binary Value.
Values are
1010011
1000101
1101100
1000110
1010110
1000110
1001101
0111101
0111101
Totally encrypted message requires 63 bits.
Consider the Cover Image, which is a gray scale Image
Example: - Consider the pixels 255, 15…..
Binary values of Pixel are
255 = 11111111
15 = 1111
LSB of each pixel is modified by the binary values of encrypted message which results in Stegano Image. This Stegano image is added to the video file as Cover Art and transmitted through network. The video created is just a collection of very small length videos and contain the information about key, i.e., 63 and Base 64 are embedded in the video may be as subtitles of video or few clues are left for the receiver.

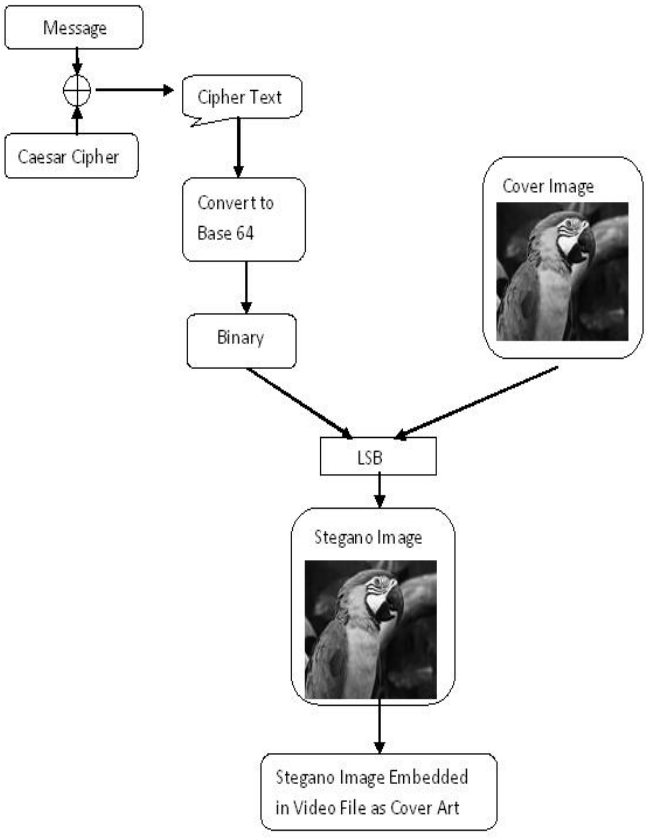

Figure: 1

Table: 1 Base 64 Character Values

M								**a**								**n**							
77								97								110							
0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
19				22				5				46											
T				W				F				u											

The example illustrates Base64 encoding converts 3 octets into 4 encoded characters.

Table: 2 Base 64 index table

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

When the number of bytes to encode is not divisible by 3 (that is, if there are only one or two bytes of input for the last block), then the following action is performed: Add extra bytes with value zero so there are three bytes, and perform the conversion to base64. If there was only one significant input byte, only the first two base64 digits are picked, and if there were two significant input bytes, the first three base64 digits are picked. '=' characters might be added to make the last block contain four base64 characters.

As a result: When the last group contains one octet, the four least significant bits of the final 6-bit block are set to zero; and when the last group contains two octets, the two least significant bits of the final 6-bit block are set to zero.

C. Decryption at Receiver Side:

Watch the Video File to obtain Key. The Key value is nothing but the number of binary digits in Encrypted Message by Ceaser Cipher and base 64.

The 5 octets are encoded into 9 encoded letters. i.e., SElFVFM== which is nine letters. ASCII value of each letter requires 7 bits.

Totally, DEATH word requires 63 bits.

The number 63 and Base 64 are inserted into video. It can be identified only by receiver.

The key values are retrieved from Video file by watching it.

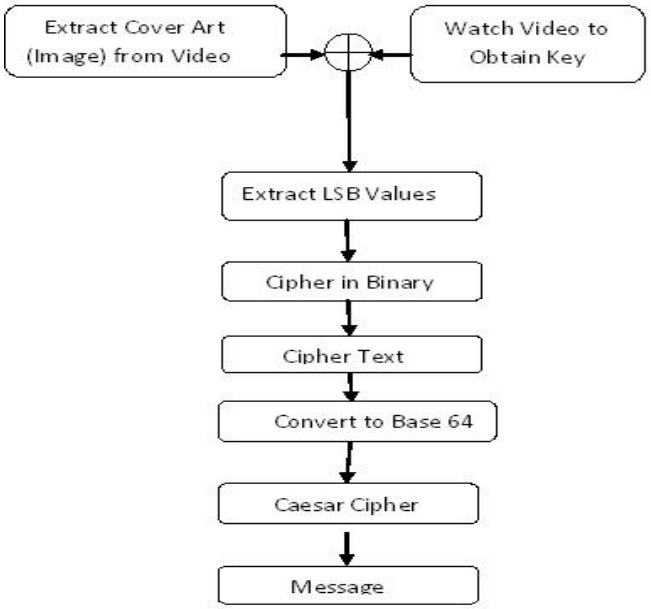

Figure: 2

Algorithm
Input: Video File (Message Encrypted in Video file)
Output: Decrypted Message
Method:

a) Watch the Video to obtain key.
b) Extract Stegano image embedded in Video file as Cover Art.
c) Extract LSB of k number of pixels of Stegano image.
d) Convert the extracted binary digits ASCII value.
e) Convert to BASE 64.
f) Apply Ceaser Cipher.
g) Convert the Decimal value to Character which is final decrypted message.

IV. BENEFITS

As LSB techniques uses JPEG images, since they use Lossy compression. In a JPEG image for hiding the data there is the need of very large cover image. The Cover Art Image is compressed to 2KB Size. Embedding this image will not have much effect to video file. For Hacker it is just video file, and only tries to apply video Steganography method. So the approach is highly secure, prevent from vulnerability.

V. CONCLUSION

Image steganography is used for the transportation of high level or top secret documents between international governments also it allows for copyright protection on digital files using the message as a digital watermark. Image steganography has many legitimate uses as it can be used by hackers to send viruses and Trojans to compromise machines. Ensuring data security is a big challenge for computer users. In this paper, the proposed method for embedding message in

image, and in turn the image is embedded in video file as cover media. Only few video file support the Cover Art. Covert Art supports a very few video file extensions, they are MP4, WMV, MOV and M4a. The stego multimedia produced by described method is highly secured and prevent from vulnerability attacks.

VI. ACKNOWLEDGMENT

I express my whole hearted gratitude to Mrs. A Santha Rubia, Assistant Professor, helped me in doing the paper. I take it as a highly esteemed privilege in expressing my sincere gratitude to my respectable personalities who helped throughout my career. My thanks and appreciations also go to my colleague people who have willingly helped me out with their abilities.

VII. REFERENCES

[1] Domenico Bloisi and Luca Iocchi, "Image based steganography and cryptography", International conf. on computer vision theory and applications(VISAPP), Italy, 2007.

[2] Niels Provos and Peter Honeyman, "Hide & Seek: An Introduction to Steganography:" IEEE Security & Privacy Magazine, May/June 2003, pp. 32-44.

[3] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, " Steganography and steganoanalysis : Different approach", in IJCITAE, vol 2, No 1, June 2008.

[4] Manoj T H, Vimalanathan P, A Santha Rubia and R Srividya, " Secured way of encrpted message transmission using audio file", in IJCTA,Volume III, July 2012, pp. 1463-1466.

[5] Venkatraman, S, Abraham, A. & Paprzycki M. "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and computing, 2004, Vol 2, pp.347-351.