Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Confidential Communication with the Help of Encryption in Animation Steganography

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

Abstract: ***To protect from these undesirable acts, we proposed a new system with use of Steganography and cryptography to make sure high security of the message. One hides the existence of the message and the other distorts the message itself. Here we use one of the most efficient and a secure algorithm is RSA Algorithm for encryption. Animation Steganography is a technique to hide any kind of files into a carrying Animation file. The use of the Animation based Steganography can be more eligible than other multimedia files.In animation embedding text "message" files (that can include power point slides, flash movies, wave files or video files). Animation Steganography is based on two principles. In the first one, the animation can be altered to certain extent without losing its functionality. In second one the host file's least significant bit can be changed. Animation Steganography is a popular technique of hiding message into animation file. We first encrypt our message and decoy with an efficient algorithm and then hide at random frames in animation.***

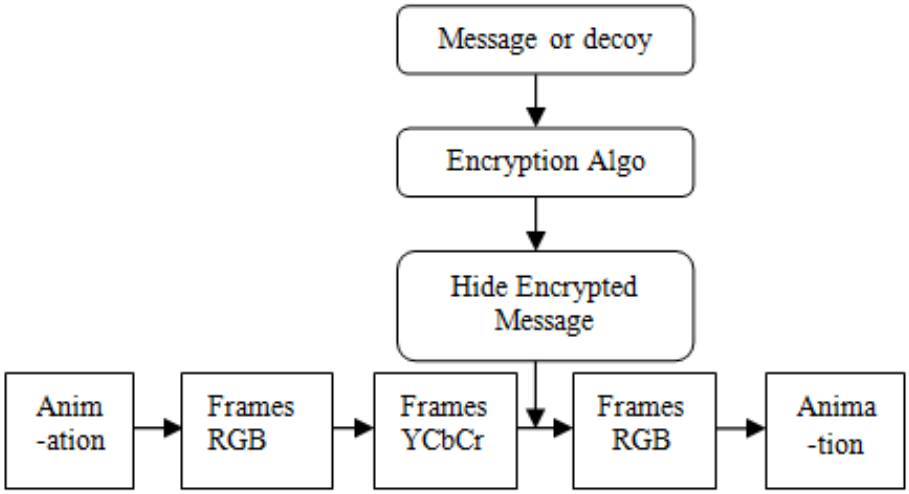
Key Words: Steganography, Encryption, Cipher, Public Key.

I. INTRODUCTION

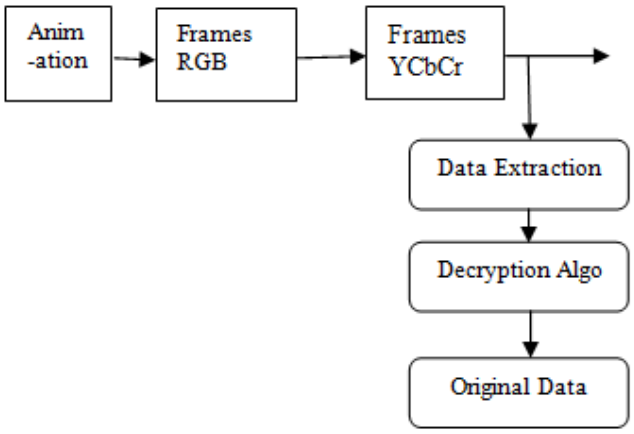
Steganography is the process of secretly embedding information inside a data source without changing its perceptual quality. Steganography comes from the Greek word steganos which literally means "covered" and graphia which means "writing", i.e. covered writing. The most common use of steganography is to hide a file inside another file [1]. Animation Steganography is a technique to hide any kind of files into a carrying Animation file. The use of the animation based Steganography[3] could be more eligible than other multimedia files, because of its size and memory requirements[3].
Here, we use RSA algorithm for message encryption. RSA algorithm is a very secure technique for cryptography. There is a chance to detection of original message after couples of attacks. Therefore, we proposed a new system with combination of steganography and cryptography.
The paper is organized as follows:
Section II describes the proposed approach of this paper.
Section III describes encryption with RSA algorithm.
Section IV describes the popular Steganography technique Animation Steganography.
Section V describes the Experimental results of my above discussed approach.

II. PROPOSED APPROACH

The block diagrams of animation encoder and decoder used to hide and extract the data are given in Figure 1.



(a) Block diagram of data hiding in animation



(b) Block diagram of data extraction from animation

Figure 1 Block diagram of data hiding and extracting in animation [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	(0010110**0**	0001110**1**	1101110**0**)
2nd Pixel	(1010011**0**	1100010**0**	0000110**0**)
3rd Pixel	(1101001**0**	1010110**1**	0110001**1**)

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	(0010110**0**	0001110**1**	1101110**0**)
2nd Pixel	(1010011**0**	1100010**0**	0000110**0**)
3rd Pixel	(1101001**0**	1010110**1**	0110001**1**)

Where, we extract least significant bits of all pixels

Encrypt message with RSA Algorithm:

- best known & widely used public-key scheme
- based on exponentiation in a finite (Galois) field over integers modulo a prime
  - nb. exponentiation takes $O((\log n)^3)$ operations (easy)
- uses large integers (eg. 1024 bits)
- security due to cost of factoring large numbers
  - nb. factorization takes $O(e^{\log n \log \log n})$ operations (hard)

RSA Key Setup:

- each user generates a public/private key pair by:
- selecting two large primes at random - p, q

- computing their system modulus N=p.q
  - note ø(N)=(p-1)(q-1)
- selecting at random the encryption key e

-where 1<e<ø(N), gcd(e,ø(N))=1

- solve following equation to find decryption key d
  - e.d=1 mod ø(N) and 0≤d≤N
- publish their public encryption key: KU={e,N}
- keep secret private decryption key: KR={d,p,q}

RSA Use:

- to encrypt a message M the sender:
  - obtains public key of recipient KU={e,N}
  - computes: $C=M^e \bmod N$, where $0 \le M < N$
- to decrypt the cipher text C the owner:
  - uses their private key KR={d,p,q}
  - computes: $M=C^d \bmod N$
- note that the message M must be smaller than the modulus N (block if needed)

III. EXPERIMENTAL RESULTS

We are using AVI (Audio Video Interleaved) format animation for hiding message and converting AVI animation into PNG (Portable Network Graphics) format image frames. We are using PNG format because it is lossless data compression we can get real data after compression.

Table I. Configuration Parameters of the Animation

Animation Properties	**Baseline Values**
Bits Per Pixel	24
Frame Rate	15
Animation Format	RGB24

Figure 2 the 17th frame of animation rofl.to30second before hide 96 bit message

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

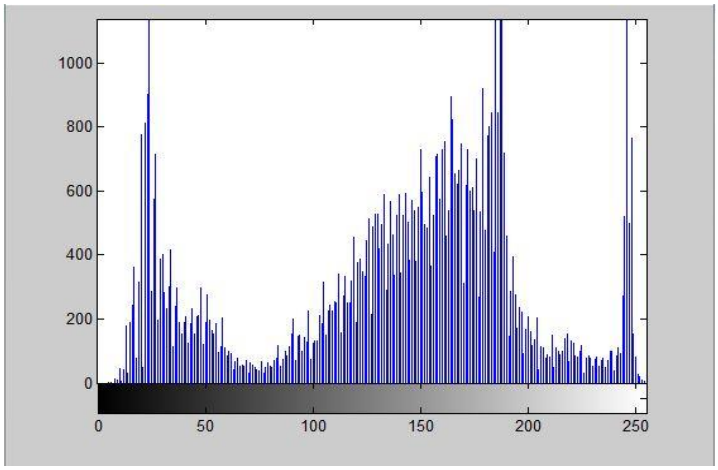


Figure 4 histogram of the 17th frame of animation rofl.to30second before hide 96 bit message

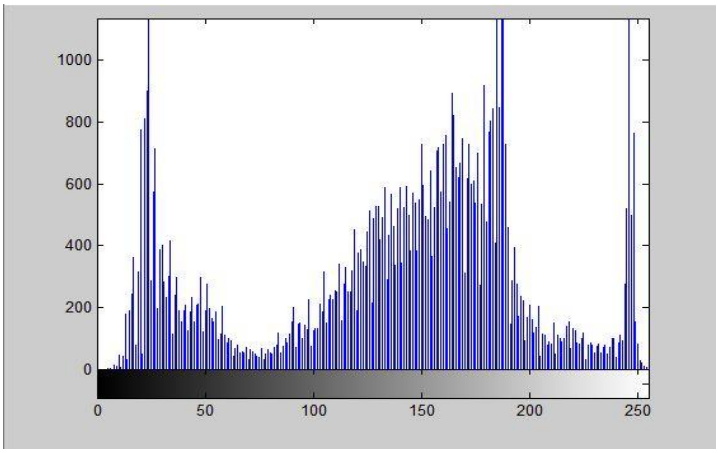


Figure 5 histogram of the 17th frame of animation rofl.to30second after hide 96 bit message

Here, we can see the difference between both histograms it means our message is successfully embedded into frames. PSNR value of above frames before message hide and after message hide is 78.3457.

IV. FUTURE WORK

An algorithm, which can decide the random positions in the frames and pixels to hide message bits, could be developed. This will further enhance this method of animation Steganography.

V. CONCLUSION

In this paper we presented a way of hiding the secret data inside the cover medium such as animation. The proposed system for data hiding uses RSA for encryption and decryption which generating public key, which results in more secure technique for data hiding. We are using random selection of frames and hide decoy with message also. The strong and weak points of these techniques are mentioned briefly so that researches who work in steganography and steganalysis gain prior knowledge in designing these techniques and their variants. The next plan is to develop a steganography technique that is robust to different types of attacks and the majority of contemporary staganlysis techniques fail to detect the presence of secret messages.

REFERENCES

[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] R. Balaji, G. Naveen, "Secure Data Transmission Using Video Steganography", International Journal of Computational Engineering Research (ijceronline.com) VOLUME 2. July-August 2012.

[3] 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, September 2012.

[4] 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.

[5] Tsutomu Matsumoto, Junji Shikata, "Authenticated Encryption and Steganography in Unconditional Security Setting", 0-7803-9491-7/05/$20.00 ©2005 IEEE.

[6] Dhawal Seth, L. Ramanathan, Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010.

[7] Ross J. Anderson, Fabien A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998

[8] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography", www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013.

[9] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. Handbook of Theoretical Computer Science 1. Elsevier.

[10] Liddell and Scott's Greek-English Lexicon. Oxford University Press. (1984).

[11] a b c d e f g AJ Menezes, PC van Oorschot, and SA Vanstone, Handbook of Applied Cryptography ISBN 0-8493-85237.

[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] Neil F. Jonhson and Stefan C. Katzenbeisser, "A survey of steganographic techniques", *Artech house.*

[14] Ross J. Anderson, Fabien A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.

[15] 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.

[16] 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.

