ISSN:0975-9646

An Approach to Secure Larger Size Data with Authenticity and Integrity

Sanjive Tyagi[1], Ajay Agarwal[2], Ramveer Singh[3]

[1] Mr.Sanjive Tyagi, Radha Govind Engineering College, Meerut, U.P.(India),
E-mail: tosanjive@gmail.com

[2] Dr.Ajay Agarwal, Prof. & Head of Department, Deptt. Of M.C.A., K.I.E.T, Gzb., U.P.(India),
E-mail: ajay.aagar@gmail.com

[3] Mr.Ramveer Singh, R.K.G.I.T, Gzb., U.P.(India),
E-mail: ramveersingh_rana@yahoo.co.in

***Abstract*— The scenario of present day of information security system includes confidentiality, authenticity, integrity, non-repudiation. This present paper focus is enlightening the technique to secure data or message with authenticity and integrity. The security of communication is a crucial issue on World Wide Web (internet) and within organizations. It is about confidentiality, integrity and authentication during access or editing of confidential internal documents. We are using a non-conventional steganography to increase security, which uses the cryptography to encrypt confidential message with the public and private keys. These keys are generated differently. Then loss-less compression takes place, which makes possible to hide larger amounts of information and documents using steganography.**

This paper presents a technique for constructing and implementing new algorithm based on embedding efficiently a large amount of data with high quality of encryption techniques, together with steganography, providing authentication and electronic documents integrity.

***Keywords*— Cryptography, Stegnography, Authentication, Integrity, Image File.**

I. INTRODUCTION

Steganography is a technology that embeds a confidential message or image within a text, or a digital picture or digital videos or digital audios. It is sometime confused with cryptography, not in name but in the usage. The simple way to differentiate that steganography conceals not only the contents of the message but also the mere existence of a message from an observer so there is no chances of doubt of the existence of the message, where as in cryptography the purpose is to secure communication from hackers by converting confidential message into not understandable form. It is observed from previous experience that sending encrypted information may create suspicion while invisible information will not do so.

Steganalysis is a technology which determines the presence of a hidden message or image in cover image and attempt to disclose the actual contents of this message [1].A more sophisticated method of steganography is by combining the two technologies to produce more security to confidential data communication such that if hackers detect the presence of data even then message cannot be decode without the knowledge of private key.

The most common stego method is the LSB approach, or Least Significant Bit. As we know digital pixels are represented by three colors: red, green and blue. These colors together form digital pictures or video. Each color of every pixel requires 1 byte of information, or 8 bits. Since the first bit is the "least significant" or carries the least amount of importance in the byte, this steganographic technique chooses to overwrite the first bit of successive bytes until the entire secret message is embedded into the original source file, or the cover data. Since we have only modified the least significant bits of a portion of the source file, the human eye should not be able to detect the degradation in the picture or video [2].

II. PRELIMINARIES

A. Stegnography:

Steganography is a technique used to embed secret information into non-secret information, preventing the message from being detected by non-authorized people.[3]

The purpose of steganography is to hide the very presence of communication by embedding messages into innocuous-looking cover objects, such as digital images. To accommodate a secret message, the original cover image is slightly modified by the embedding algorithm to obtain the stego image. The embedding process usually
incorporates a secret stego-key that governs the embedding process and it is also needed for the extraction of the hidden message [4].

There are three basic views behind hiding information. The first is capacity, which is the amount of information that can be embedded within the cover file. An information-hiding algorithm has to be able to compactly store a message within a file. Next is security, which refers to how a third-party can detect hidden information within a file. Intuitively, if a message is to be hidden, an ideal algorithm would store information in a way that was very hard to notice. High security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too. Various encryption

techniques like cryptography, digital watermarking, steganography etc have already been introduced in attempt to address these growing concerns [5].

Steganography have four application areas:

- Copyright Protection. It has security, invisibility and robustness requirements. Watermark techniques fit in this area.
- Authentication. It has security and invisibility requirements. Digital signature fits in this area.
- Secret and Invisible Communication. It has requirements for security, invisibility and insertion of high volumes of secret data. [6]

B. Cryptography

Cryptography is a branch of applied mathematics that aims to add security in the ciphers of any kind of messages. Cryptography algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. The data integrity aims to verify the validity of data contained in a given document. [7]

There are of course a wide range of cryptographic algorithms in use. The following are amongst the most well known: DES 'Data Encryption Standard'. This is a cipher that operates on 64-bit blocks of data, using a 56-bit key. It is a 'private key' system.

RSA: RSA is a public-key system designed by Rivest, Shamir, and Adleman.

HASH: A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest', or a 'fingerprint'.

AES: This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST etc. [8]

C. Data Compression

Previous well known data compression techniques includes the standard algorithm for example, Huffman coding is an entropy encoding algorithm used for lossless data compression. The term refers to the use of a variable-length code table for encoding a source symbol (such as a character in a file) where the variable-length code table has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol. It was developed by David A. Huffman. There are various data compression algorithm like Run-length encoding, Burrows-Wheeler transform, Dynamic Markov Compression, entropy encoding: Huffman coding ,Adaptive Huffman coding, Shannon-Fano coding, arithmetic coding etc., which has been used for data compression successfully internationally.

In addition, to avoid sending files of the enormous size, a compression scheme can be employed what is known as lossless compression on secrete message to increase the amount of hiding secrete data, a scheme that allows the software to exactly reconstruct the original message. [1]

So, in order to obtain more security in our described or prescribed method, that secrete message is encrypted and to hide large amount of data some appropriate compression technique is used then we have embedded encrypted and compressed message into cover image.

.

III. OUR APPROACH

Due to the rapid progress of computer and network technique, we are becoming more and more capable of enjoying to enhance the degree of security. Steganography is method to hide the confidential data/image. In networking, at the time of data transmission, hackers can track of suspicious image then they could get the hidden image by applying some complex mathematical operation. So there are chances of confidential information or being snooped.

According to our new concept, we encrypt the original text message letter by letter applying a function, which involves certain mathematical operation using corresponding letters and also numbers from the original image, then we use strong RSA algorithm to generate the public key and private key. For encryption we need to use public key for plain text M and mathematical operation called multiplicative module in between text or message and public key i.e

Cipher Text: $C = M^e \pmod r$.

Then using appropriate compression algorithm on secrete data file (c) to hide a larg amount of data with high security.

Then Hide compressed and encrypted text into cover image using Stegnography algorithm i.e List Significant Bit (LSB) coding is the way to embed information in cover image file. In this LSB technique is applied on compressed encrypted message. It is really appreciable method to provide high security to the high confidential image.

The proposed method is enhanced or characterized by robustness, larger amount of secrete data, less time complexity and especially high security.

Proposed work deals with the security of text message by applying asymmetric key cryptography algorithm in which we use public and private key. Public key is used at sender side and private key used at receiver side. Public key and private key are always unique using RSA algorithm with modification that a mathematical function Ø. This function using a value depends on the decimal value of the R array of each pixel of cover image. The first letter corresponding to the first pixel and next to the second pixel and so on .

A mathematical function Ø is using R array of each pixel of cover image for generating the Public Key KU={e, r} and Private Key KR={d, r}.The encrypted code is taken digit by digit This approach constitute the phase one security in our work.

Now in the second phase of work, we have used some loss less compression technique to compress the encrypted text so that we can hide large amount of data in cover image.

In next phase, we have introduced the hiding of encrypted and compressed text file into any cover image.

We have designed new algorithm. This algorithm follows some rules to generate the private key and public key.

Rules:

(a) Generate a prime number n, where ln is the highest number assigned to the alphanumeric character (if ASCII is used) then n is taken randomly prime number greater than ln.

(b) Here m is taken from the decimal value of the R array of the pixels of the original cover image such that any prime number in the decimal value less than n.

In our work private key and public key are always unique because we are generating randomly prime number based on the confidential message text and original cover image. This method is a unique to generate prime number such that no one can guess the prime number to crack the public and private key.

We are using new method to convert the text into number system that is a mathematical function Ø is used which gives the number of prime numbers below given number say p.

A. Algorithm for encrypting the confidential message and generating public key and private key

Step 1:
Convert the text to number system, which are ASCII number of character.
Step 2:
A mathematical function Ø is used which gives the number of prime numbers below given number say p.
Step 3:
Here, the value of p depends on the decimal value of character of cipher text.
Step 4:
The Ø function is then added or subtracted from the number by checking the parity of decimal value of character of cipher text.
AC=ASCII Converted Character numbers of confidential Message.
RC=Decimal value of the R array of the pixels the original cover image.
RsC=Result value after applying the Ø function
Now, Using Ø function AC are converted as
AC- Ø (RC) = RsC
AC+ Ø (RC) = RsC
Step 5:
Now using two prime number m and n generate public key and private key
Calculate, r = n * m
Where n and m both prime number, n ≠ m
Calculate f (n) = (n-1) (m-1)
Step 6:
Select integer e
gcd(f(n),e)=1; 1<e<f(n)
Step 7:
Calculate $d = e^{-1} \bmod f(n)$
Step 8:
Public Key KU = {e, r}
Private Key KR= {d, r}
Step 9:
Encryption using public key
Plain Text M
Cipher Text: $C = M^e \pmod r$
Step 10:
Perform the compression on cipher text using appropriate compression algorithm to increase the amount of hiding secrete data.
Step 11:
Perform Steganography on compressed encrypted text into any cover image.

B. Algorithm to embed confidential message into cover image file.

Algorithm to embed confidential message into cover image file named inFile generate new file with embedded message file named outFile.
Encoded-Message (msg,inFile on input-mode,outFile on output-mode)
Step 1:
Read offset bytes from input inFile and writes to output File outFile
Step 2:
Calculate message length and write it into output file by embedding it in last two bits for every byte. Message length being 16 bits, will be stored in 8 pairs of 2 bits.
Step 3:
Embed each byte of message in 4 pairs of 2 bits each is embedded in 4 byte of input file and written into output file named outFile.
Step 4:
Write the remaining bytes of the input file into output file.

C. Algorithm for Decryption of message from Image

The picture is received at receive side. Perform decryption from cover image to obtain the hidden message at receiver side. This function decode message from a file named outFile open on output mode.
Decode Message (outFile on Input-mode)
Step 1:
Read offset bytes from the input file and discard them.
Step 2:
Read last 2 bits of consecutive 8 bytes and concatenate them to get the message length.
Step 3:

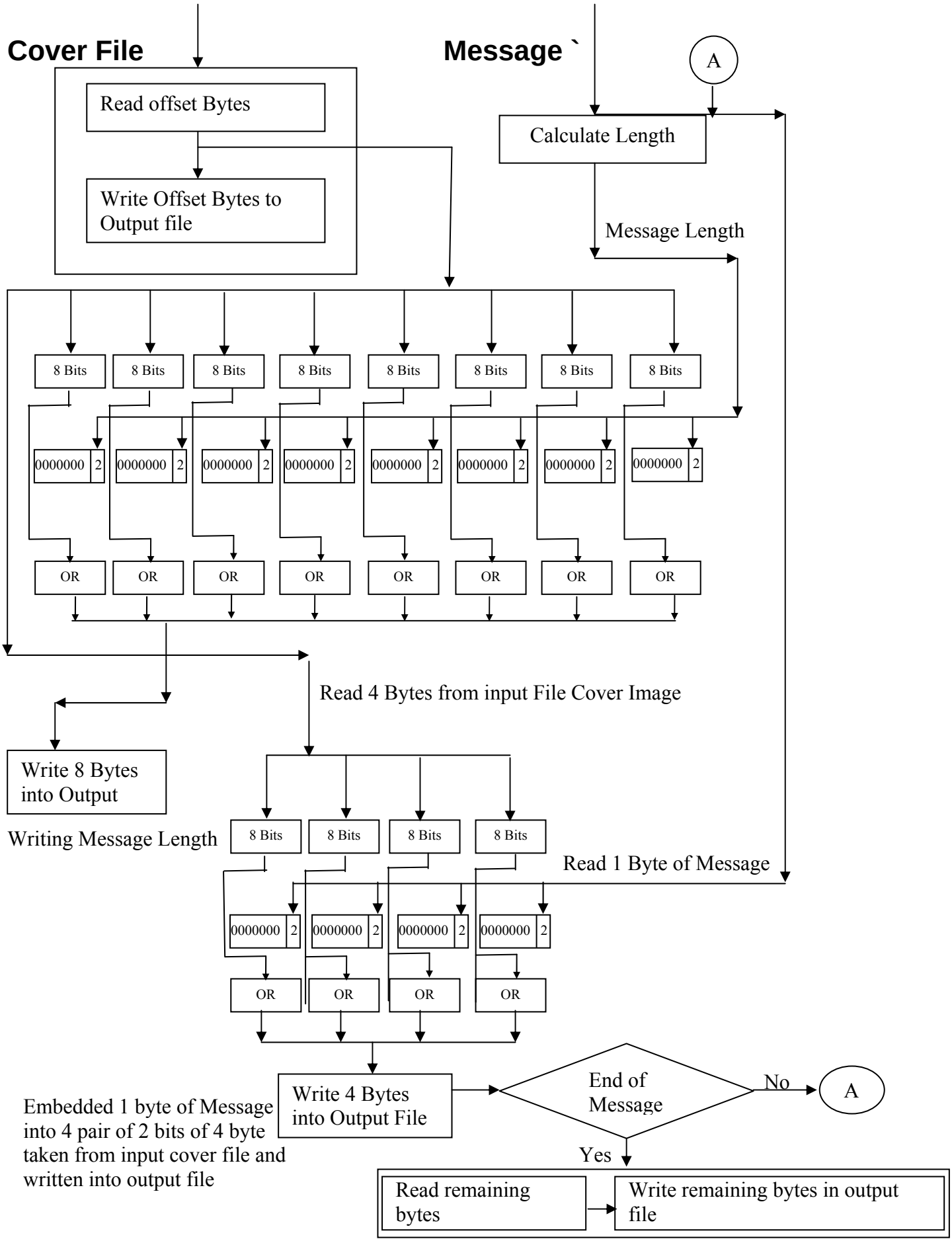

Fig. 1. Process of embed *confidential message into cover image file.*

Read last 2 bits from input file in pairs of 4 and concatenate them to get message of 1 byte.

Step 4:

Repeat step 3 until the message is extracted of calculated length.

IV. CONCLUSIONS

In this paper, we propose an innovative approach by using the LSB matching method to embed secure data into the stego-image. The result shows that it can not only keep the acceptable image quality and security but also enhance handiness for transmission in our proposed scheme. The encryption of the message increases the strength of security of hiding technique which is used in the proposed system. The cover file can be transmitted normally after hiding secure data file. Other word the cover file includes with secure data provides the two times more security than tradition encryption system.

REFERENCES

[1.] Nameer N. EL-Emam, *Hiding a Large Amount of Data with High Security Using Steganography Algorithm* Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan

[2] Alain C. Brainos, A Study Of Steganography And The Art Of Hiding Information, East Carolina University, http://www.infosecwriters.com/text_resources/pdf/steganographyDTEC6823.pdf

[3] Niels Provos, Peter Honeyman, *Hide and Seek: Introduction to Steganography,* **IEEE Security and Privacy,** Volume 1 , Issue 3 (May 2003), Pages: 32 - 44

[4] Jessica Fridrich and Miroslav Goljan, *Digital image steganography using stochastic modulation*, Department of Electrical and Computer Engineering, SUNY Binghamton, Binghamton, NY, 13902-6000, USA.

[5] Swarnendu Mukherjee, Swarnendu Bhattacharya, Amlan Chaudhury *Triple Layer Data Security* ACM Ubiquity, Volume 9, Issue 17, April 29-May 5 ,2008

[6] Zhao, J. *In business today and tomorrow,* ACM Communications of the ACM, p. 7, 1998.

[7] Diego F. de Carvalho, Rafael Chies, Andre P. Freire, Luciana A. F. Martimiano and Rudinei Goularte, *Video Steganography for Confidential Documents: Integrity, Privacy and Version Control* , University of Sao Paulo – ICMC, Sao Carlos, SP, Brazil, State University of Maringa, Computing Department, Maringa, PR, Brazil.

[8] Alfred J. Menezes, Paul. C. Van *A handbook of cryptography*