DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5926

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

EFFICIENT SECURITY FRAMEWORK FOR DATA INTEGRITY AND DATA ACCESS IN CLOUD ENVIRONMENT

J. Kumaran Kumar
Assistant Professor in Computer Science and Engineering,
Pondicherry Engineering College,
Puducherry, India

V. Bhuvaneswari
PG Student,
Pondicherry Engineering College,
Puducherry, India

Abstract: Cloud computing is a highly emerging area in the market and provide the way of mechanism for global challengers. The priority of Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers. This paper attempts a combination of cryptography andsteganography, which provides a big determination for its security. The secret message can be encrypted before its actual process. The main goal of this work to hide a secret message into pixels of the image so that the hacker does not difference between the original and steganography image. The embedding can be using LSB techniques. Steganography can be replaced by unused bits in the data (such as graphics, sound, audio, video, text). The existing work, AES algorithm can be used to cryptography. The hackers can easily to theft the information due to the insecure links. To overcome this problem to implement the F5 matrix encoding to improve the efficiency of embedding. This present work focuses on enlarge the technique to secure text, video, audio, image with authenticity and integrity.

***Keywords*:** Cloud Computing, Data Integrity, Confidentiality, F5 implementation, Steganography, Matrix Encoding.

1. INTRODUCTION

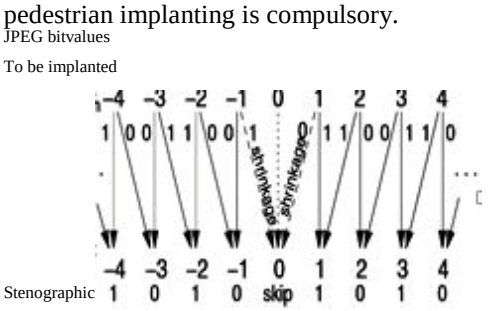
Cloud computing is an element by which service and sharing resources through over internet. It is a combination of virtualization, grid computing, web services, etc. The internet is insecure because everyone can access and information extensive open. Cryptography or steganography are keep sensitive data due to data communication through internet. Steganography is to hiding a secret message via audio, image, text and video [1]. Data integrity is consists of information integrity in the cloud. The unauthorized person cannot access or modified the data[2]. Authorization only authorize person to access the data, unauthorized person does not access the data. Data integrity to provide the service such as SaaS, PaaS, IaaS [3, 4].The secret message and original image is also called the cover-image, the embedding algorithm slightly changes by cover image. The main purpose of steganography to hidden a high secret message in a given medium [5]. This work aims at to develop a safe keeping in the steganography algorithm by producing a F5 matrix encoding.

The message can be embedded into DCT coefficient and minimize the length. The inputs are given to the steno image are TIFF,BMP,JPEG or GIF, output file name, secret message, password to pseudo random number generator and comment[11,12].

2. PROPOSED MODEL

The main goal of the PM to implement the F5 algorithm for advanced efficiency. Steganography is high efficiency through matrix encoding [1]. In this to prevent visual attacks resistance to statically attack (chi-square attack). Many different file formats can be used, but digital images are frequently access through internet [7].In F3 does not overwrite bits the Join Steganography, rather it decrements the coefficient's absolute values[8]. The LSB does not match not containing factor with the value zero, it cannot be decrement the total value. Hence zero factors are not used in this method [9]. The LSB of nonzero factors match the top-secret message after inserting, but the LSB is not overwritten as overwritten bits can be identified by numerical methods (Chi-Square method).

Some implanted bits fall mark to contraction. Contraction occurs every time F3 decrements the complete value of 1 and -1 producing a 0. The receiver cannot distinguish a 0 factor that is stegonagraphically idle from a 0 made by contraction. It skips all zero factors. Hence pedestrian implanting is compulsory.



The above figure 1, the histogram displays more even factors than odd factors. This is due to repeated inserting after contraction. Contraction occurs only if we surround a 0 bit. The duplication of these 0 bits shifts the ratio of stenographic values in favour of the stenographic zeros. This is undesirable and can be distinguished by numerical means. To overcome this problem to use F4 algorithm, it is also not satisfied [1]. To avoid all the problem to implement the F5 algorithm it is more effective when match to previous algorithm. JPEG method can be used to implanting method that would provide high steganography capacity without lose security[10].The F5 algorithm insert a message bits into irregular pick a DCT coefficients and matrix embedding that reduce the unavoidable number.

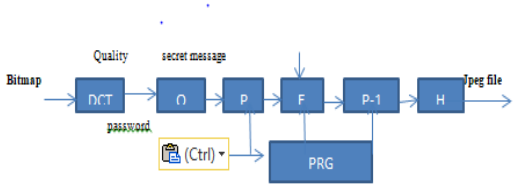


Fig.2 System Architecture of F5 Implementation

In the inserting method, the number of non- zero and non-factors are used to fix the matrix inserting, it decrease the number of adjustments of the cover-image. The inserting has three parameters (n, k, c) [6], kis the number of implanted bits and where cis the number of changes per group of n factors. In their paper [11], the writers define a modest matrix inserting (1, 2k–1, k) using a "hash" determination that outputs kbits when useful to 2*k*–1 factors.

The inserting method start with PRNG from the user PIN and making an arbitrary number via the DCT factors of the cover image. The PRNG is also used to encode the value *k* using a stream cipher and implanted the message length in the start of the message stream [10]. The contented of the message is embedded using matrix inserting, inserting *k* message bits into one group of 2k–1factors by decrementing the absolute value of at most one factor from each collection by one.

The following steps are used in F5 implementation:

1. Become the RGB illustration of the input image.
2. To Compute the superiority factor *Q* and wrapping the image to loading the quantized DCT factors.
3. To calculate the assessed size

C = hDCT– hDCT/64 – h(0) – h(1) + 0.49h (1)

4. The PIN is used to make an idea for a PRNG that defines the arbitrary message bits. It is also used to produce a quasi-arbitrary bit-stream that is XOR with the message to form anarbitrary bit-stream. DC factors and factors equal to zero during the insertingmethodare avoided.
5. The message is separated into sectors of kbits that are surrounded into a group of2k–1 factors. If the has hing value does not equal the factor message bits, the exact value of the factors is reduced by one to contact an individual value. If the factor becomes zero, the event is called contraction, and the similar k message bits are re-implanted in the next group of DCT factors.
6. If the message size is capable the assessed capacity, the inserting process can be proceeds, then the error message can be created the maximal potential length.

3. RESULTS AND DISCUSSIONS

The embedding process consists of the sequential substitution of each Least Significant Bit (LSB) of the image pixel for the bit message.

1st Step: Convert the data from decimal to binary.

[Message] $\xrightarrow{\text{DtoB}}$ [1000001]

2nd Step: Read Cover Image "baby.bmp" as shown in figure 3

144	142	146	152	147	151	157	186
160	155	159	165	133	123	133	145
144	141	141	138	61	55	79	65
120	123	131	144	50	61	74	92
170	167	167	166	61	59	59	56
120	125	131	132	61	59	59	59
124	133	136	13	131	88	76	77
138	153	167	154	139	….	…..	….

3rd Step: Convert the Cover Image from decimal to binary.

10010000	10011011	10011110	00001011	11001100	01010111
10010101	01011000	10111000	11110101	00110101	10100010
01010010	10101001	01010101	10101010	01011010	10111010
10010000	10011011	10011110	00001011	11001100	01010111
10010000	10011011	10011110	00001011	11001100	01010111

4th Step: Break the byte to be hidden into bits.

Is divided into 8 bytes

[10000001] $\rightarrow$ [1 0 0 0 0 0 0 1].

5th Step: Take first 5 byte of original data from the Cover Image.

10010000	10011011	10011110	00001011	11001100

6th step: Replace the least significant bit by one bit of the data to be hidden.

- First byte of original data from the Cover Image

1	0	0	1	0

- First bit of the data to be hidden

1

- Replace the least significant bit

1	0	0	0	0

- Repeat the replace for all bytes of Cover Image.
- Finally the cover image before and after steganography.

In this method, to hide a message up to 65536 bytes. The message can be embedded into LSB of the system. To protect the external significance such as noise, compression, filter and so on.

In F5 steganography, the message with transfer to 1736 bits means and compressed with 459 bits. To minimize the difference between old pixel value to new pixel value in the steganography image.

To embedded K bits take place n=2^k-1.

K	N	Change density	Embedding rate	Embedding efficiency
1	1	50%	100%	2.1
2	3	25%	66.7%	2.6
3	7	12.5%	42.9%	3.5
4	15	6.25%	26.7%	4.2
K	N			>k

Using this matrix encoding technique to decrease the changes in the message. In this PM to apply the F5 algorithm with quality factor is 75 and modified coefficients number of all non-zero.

4. CONCLUSIONS

F5 algorithm has been implemented based on insecure links. It efficient addressing for insecure links and

matrix calculation. The privacy techniques help to preserve the insecure links and also matrix calculation to secure the data in hacking by hackers .The hackers do not stealing the information to provide more security using F5 algorithm.

5. ACKNOWLEDGEMENT

The authors gratefully acknowledge the authorities and Pondicherry Engineering College for the facilities offered to carry out this work.

REFERENCE

[1] Westfeld, A.: High Capacity Despite Better Steganalysis (F5–A Stenographic Algorithm).In: Moskowitz, I.S. (eds.): Information Hiding. 4th International Workshop. Lecture Notes in Computer Science, Vol.2137. Springer-Verlag, Berlin Heidelberg New York (2001) 289–302.

[2] Lee, L.: LSB Steganography: Information within Information, Journal of Computer Science, Vol(265), No (5)(2004) pages 10-14.

[3] Bailey K, Curran K. "An Evaluation of Image Based Steganography Methods" Multimedia Tools & Applications, Vol.30.No.1.pages 55-88 July 2006.

[4] Xiang-yang, L., Dao-shun,W., Ping, W., Fen-lin, L: A review on Blind Detection for Image Steganography, Journal of Signal Processing, Vol(88),Issue(9) December 2008 pages 1-4.

[5] Hengfu, Y., Xing Ming S., Guang S., A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution, Journal of radio engineering, VOL. (18), NO. (4)(2009) pages 32-38.

[6] JammiAshok"Steganography: An Overview" International Journal of Engineering Science and Technology Vol. 2(10), 2010 page 19.

[7] Harjit Singh Lamba and Gurdev Singh, ―Cloud Computing-Future Framework for emanagement of NGO's‖, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011 pages 22-24.

[8] Dr.Gurdev Singh, ShanuSood, Amit Sharma, ―CM-Measurement Facets for Cloud Performance‖, IJCA, Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, pages 304-315 June 2011

[9] Rabi Prasad Padhy, ManasRanjanPatra , Suresh Chandra Satapathy, ―Cloud Computing: Security Issues and Research Challenges‖, International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011 pages3-4.

[10] Prince Jain, Security Issues and their Solution in Cloud Computing‖, International Journal of Computing & Business Research, Proceedings of _I-Society Vol. 2(11)2012' pages 6-7.

[11] Babita and Ayushi, "Secure Image Steganography Algorithm using RGB Image Format and Encryption Technique", International Journal of Computer Science and Engineering Technology, Vol. 4, No. 6,pages 758-762 , 2013.

[12] Samer, :A New Algorithm for Hiding Gray Images using Blocks, Information , Security Journal, The Hashemite University, Jordan, Volume (15), Issue (6) 2015 pages 2-4.