IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Securing Cloud Data using Crypto-Stegno based Technique

Kirti Kini[1], Meera Mithani[2], Rinali Naik[3], Divyata Raut[4], Prof.M.K.Kumbar[5]

Dept. of I.T., JSPM's Bhivarabai Sawant Institute of Technology & Research , SPPU university, India[1,2,3,4,5]

Abstract: In our Paper, the problem of transmitting redundant data over an in Secure, bandwidth-constrained communications Channel is discussed. A content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least signicant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. Using data hiding key the receiver can extract additional data even the receiver has no information about the original image content. Using the decryption key the receiver can extract data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryptions key, the receiver can extract the additional data and the original image without any loss.

Keywords: Content owner, data-hider key, decryption key.

I. INTRODUCTION

The reversible data hiding in encrypted images, all previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. So the proposed method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image.

Cloud computing is an architecture for providing computing services via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers. Service providers offers cloud platforms for their customer to use and create their web services, much like internet service providers offer customer high speed broadband to access the internet. There are numerous security issues for cloud computing as it encompasses many technologies. Security issues in cloud computing consists of application, platforms and infrastructure segment. Each segment performs different operations and offer different products for business and individuals around the world. The business application includes saas utility computing, web services, pass managed service providers, service commerce and internet integration. The cloud computing encounters various security issues, as it comprises of many technologies namely, networks, database, operating systems, virtualization, resources scheduling, transaction management, load balancing, concurrency control, memory management..Therefore security issues for many of these systems and technologies are applicable to cloud computing

Paper Objective:

The objective of this paper is to provide an efficient data hiding technique and image Encryption in which the data and the image can be retrieved independently. The aim or objective of the project is to implement a reversible data hiding technique in encrypted images.

The proposed technique or method can achieve real reversibility, that is, data extraction and image recovery are free of any errors.

Need:

1. To overcome the existing system of watermarking.
2. To provide double layer encryption.
3. Security for data.

II. EXISTING SYSTEM

1) Separable Reversible Data Hiding using RC4 algorithm:

Authors: V.Suresh , C. Saraswathy

A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though the receiver does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. Two key weaknesses were discovered within a year for the RC4 algorithm. RC4 is a stream cipher that means it essentially generates a Pseudorandom Streams of bits (key streams) which is combined with plain text using bit-wise Exclusive OR for the encryption process.

The decryption process is the same way as encryption and encrypted message will be combined with the same key streams using bit-wise Exclusive OR. Due to the symmetric property of the XOR the plain text will be recovered from the cipher text without any error. Although RC4 is popular and fast due to its short and simple PRGA (core) algorithm but several weaknesses have been found in KSA stage of RC4. Thus, we have decided to study on this matter in order to come up with a solution to improve RC4 algorithm, in which it was necessary to make KSA

DOI 10.17148/IJARCCE.2016.5345

much more complicated so that it could be against the attacks. [7]. In this study we have applied a new symmetric algorithm called FJ RC-4, which is derived from RC4. Our studies shown that KSA is the vulnerable stage of RC4, whereas a new self-developed symmetric algorithm, FJ-RC4, has tried to increase the security of RC4 by introducing the new algorithm for the KSA stage. We have researched and compared the robustness of the RC4 and FJ-RC4 and shown that FJ-RC4 is stronger than RC4 against the attacks. In addition, it takes more time to find key in FJ-RC4 and requires more resources. Thus, FJRC4 is more secured algorithm than RC4 algorithm.

2)Separable Reversible Data Hiding in Encrypted Image:

Authors: X. Zhang

This technique proposes a novel scheme for separable reversible data hiding in encrypted images. The scheme proposed in this paper is made up of encryption of image, data embedding and recovery of original image phases. The sender also known as the content owner encrypts the original uncompressed image using the image encryption algorithms using a key known as the encryption key to produce an encrypted image.

Then, the server compresses the least significant bits (LSB) of the encrypted image using a data-hiding key for creating a sparse space to store the additional data or the watermark information. At the destination side, the data embedded in the image can be retrieved easily from the encrypted image containing additional data according to the data-hiding key. Since the embedding of data only affects the LSB, a decryption of the image with the encryption key can result in an image that is similar to the original version of the image. When we use both keys i.e. the encryption and data-hiding keys, the additional data embedded can be extracted successfully and the original image can be recovered perfectly by exploiting the spatial correlation in natural image. The disadvantages of this technique were eliminated by proposing a new scheme known as the securing cloud data through crypto-segno based techniques. [13]

III.PROPOSED METHODOLOGY

FJRC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plain-text used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table.

The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though the receiver does not know the original content. With and encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key.

A .Key Schedule Algorithm

In FJ-RC4 at beginning of the process the main key is divided by three equal portions to make three different sub-keys. If the length of main key is not divisible by three, then we use zero padding to make it divisible by three Fill third array of the same size with the key.

In the FJRC4 the string message that is supposed to be locked for the. encryption will be combined with the first sub-key array, array[0], using bit-wise Exclusive OR for the first stage of encryption process. The result from this step will be combined with the second sub-key array, array[1], using bitwise Exclusive OR for the second stage of encryption process. Finally, the result from step 2 will be combined with the third sub-array, array[2] , using bit-wise Exclusive OR for the third stage of encryption. The third encryption process will produce the cipher string by the FJ-RC4

Layer 1 Encryption:

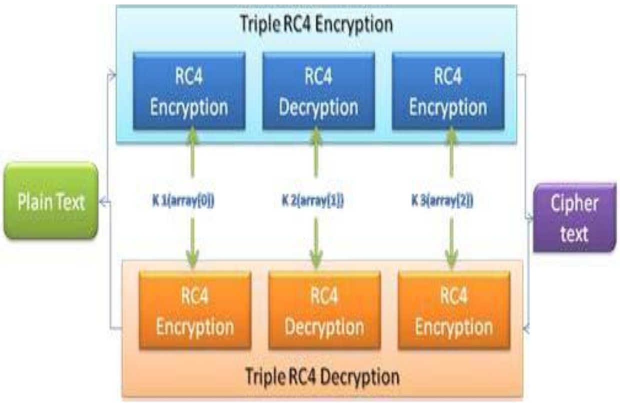

Fig.1.1 FJRC4 Encryption-Decryption Algorithm

B. Decryptions

It should be mentioned that bit-wise Exclusive OR operation has symmetric property and original string can bare covered from the encrypted string using the cipher string that has been encrypted by FJ-RC4. Since the main key is divided by three portions during the encryption process, thus the decryption process is in the opposite direction of the encryption process.

First, the cipher string must be combined with the third sub-key array using bit-wise Exclusive OR for the first stage of decryption. The result from this step will be combined with the second subkey array using bit-wise Exclusive OR for the second stage of decryption. Finally, the result from step 2 will be combined with the third sub-array, using bit-wise Exclusive OR for the third stage of decryption. Thus, third decryption process will produce the original string by the FJ-RC4. .

The Encryption And Decryption Algorithm is shown in Fig 1.1.

Layer 2 Encryption:

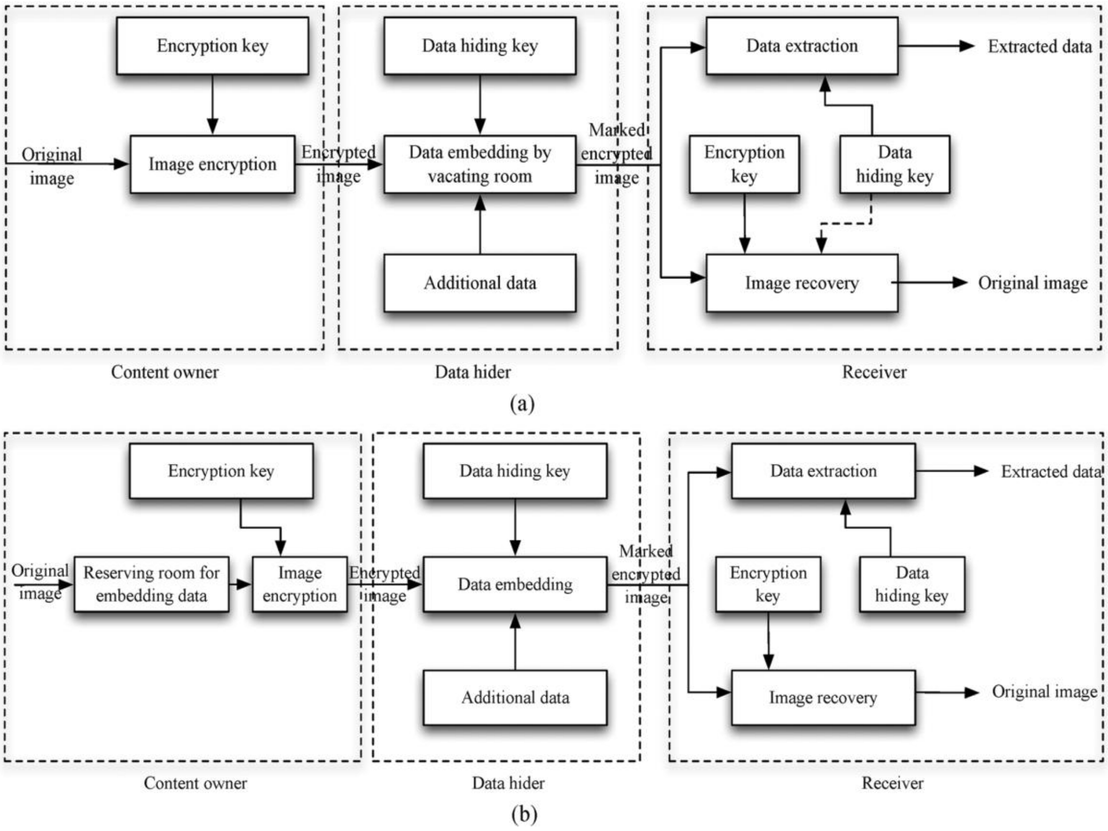

Fig.1.2. Framework: “vacating room after encryption (VRAE)” versus framework: “reserving room before encryption (RRBE).” (Dashed line in (a) states that the need of data hiding key in image recovery varies in different practical methods). (a) Framework VRAE. (b) Framework RRBE.

IV.CONCLUSION

Pseudo random sequence consists of random bits generated using the encryption key. In our system we are using FJRC-4 algorithm is used to create the pseudo-random sequence using the 128-bit encryption key. The additional data inserted to encrypted image using the parameters. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. Compared with the other algorithms, the proposed system demonstrated successful accuracy in recovering the original images. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

REFERENCES

[1] T. Kalker and F.M.Willems, “Capacity bounds and code constructions for reversible data-hiding,” in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[2] W. Zhang, B. Chen, and N. Yu, “Capacity-approaching codes for reversible data hiding,” in Proc 13th Information Hiding (IH’2011), LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

[3] W. Zhang, B. Chen, and N. Yu, “Improving various reversible data hiding schemes via optimal codes for binary covers,” IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[4] J. Fridrich and M. Goljan, “Lossless data embedding for all image formats,”in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA,Jan. 2002, vol. 4675, pp. 572–583.

[5] J. Tian, “Reversible data embedding using a difference expansion,”IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.

[6] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[7] V. Suresh and C. Saraswathy, “Separable Reversible Data Hiding Using Rc4 Algorithm,” 2014 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22.

[8] X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[9] P. Tsai, Y. C. Hu, and H. L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Process., vol. 89, pp. 1129–1143, 2009.

[10] L. Luo et al., “Reversible image watermarking using interpolation technique,”IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[11] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” IEEE Trans.Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.

[13] X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

DOI 10.17148/IJARCCE.2016.5345