ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 216 – 219 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

Data Hiding As Encrypted Image

[1]SK.Gouse Pasha, [2]Ravi Regulagadda,

Department of Computer Science Engineering

[1]Mallareddy Institute of Engineering and Technology, Hyderabad, AP, India

[2]Mallareddy Institute of Engineering and Technology, Hyderabad, AP, India

gousepasha@live.com, ravi.regulagadda@gmail.com

ABSTRACT- Data hiding is a method to cover knowledge representing some information. By this method, we can achieve real reversibility, separate data extraction. We reserve room before encryption with a traditional RDH algorithm. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error. This method can embed more than 10times as large payloads for the same image quality as the previous methods. Encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content. Reversible Data hiding in encrypted Images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. It is easy for the data hider to reversibly embed data in the encrypted image.

Key Words: Image encryption, image recovery, image extraction, reversible data hiding.

I. INTRODUCTION

DATA Hiding is spoken as a method to cover knowledge (representing some information) into cowl media. That is, the information hiding method links two sets of knowledge, a group of the embedded knowledge and another set of the duvet Media knowledge. The relationship between these two sets of knowledge characterizes totally different applications. for example, in covert communications, the hidden knowledge might typically be immaterial to the duvet media. In authentication, however, the embedded knowledge is closely associated with the cover media. In these two sorts of applications, physical property of hidden knowledge is a very important demand. In most cases of data Hiding, the duvet media can expertise some distortion due to knowledge Hiding and can't be inverted back to the first media. That is, some permanent distortion has occurred to the cover media even once the hidden knowledge are extracted out. In some applications, like diagnosing and enforcement, it is crucial to reverse the marked media back to the original cowl media once the hidden knowledge are retrieved for some legal issues. In alternative applications, like remote sensing and high-energy particle physical experimental investigation, it is additionally desired that the first cowl media will be recovered as a result of the specified high-precision nature. The marking techniques satisfying this demand are spoken as reversible, lossless, distortion-free, or Reversible knowledge Hiding facilitates large risk of applications to link two sets of knowledge in such some way that the cover media will be lossless recovered once the hidden knowledge have

ISSN 2278-3091
International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 216 – 219 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

been extracted out, so providing an extra avenue of handling two totally different sets of knowledge. Obviously, most of the present knowledge Hiding techniques are not reversible. The well-known least important bit plane (LSB) based mostly schemes are not lossless owing to bit replacement while not memory.

Encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

II. PROPOSED WORK

- This method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.
- This method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.
- This 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.
- We can achieve real reversibility, that is, data extraction and image recovery are free of any error.

III. ADVANTAGES

- This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.
- It is easy for the data hider to reversibly embed data inthe encrypted image.
- This method can embed more than 10 times as large payloads for the same image quality as the previous methods.

In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digits further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.[1] It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2 (such as in 2^{31}...20). Although a few CPU manufacturers assign bit numbers the opposite way (which is not the same as different), the term LSB (of course) remains unambiguous as an alias for the unit bit.

By extension, the least significant bits (plural) are the bits of the number closest to, and including, the LSB.

The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000 to 000).

ISSN 2278-3091
International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 216 – 219 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

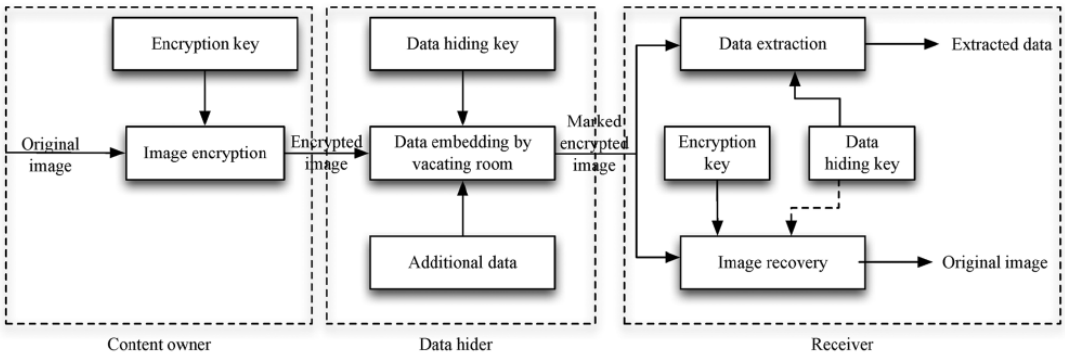

Fig1. Reversible Data Hiding

IV. RESULT

By this method we can achieve real reversibility, that is, data extraction and image recovery are free of any error. It is easy for the data hider to reversibly embed data inthe encrypted image. This method can embed more than 10 times as large payloads for the same image quality as the previous methods.

V. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

VI. REFERENCE

[1] T. Kalker and F.M.Willems, “Capacity bounds and code constructionsfor 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 forreversible 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 datahiding 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, Securityand 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] D.M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible

watermarking," IEEE Trans. Image Process., vol. 16, no. 3,pp. 721–730, Mar. 2007.

[8] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarkingbased 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 schemeusing predictive coding and histogram shifting," Signal Process., vol.89, pp. 1129–1143, 2009.

[10] L. Luo et al., "Reversible imagewatermarking 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, "Reversiblewatermarking 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 ofApplied Cryptography. Boca Raton, FL, USA: CRC, 1996.

[13] K. Hwang and D. Li, "Trusted cloud computing with secure resourcesand data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22,Sep./Oct. 2010.

[14] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, "On compressing encrypted data," IEEE Trans. SignalProcess., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.