ISSN 2320 – 2602

Volume 4 No.4, April 2015

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/ijacst/static/pdf/file/ijacst10442015.pdf

INFORMATION SECURITY WITH IMAGE THROUGH REVERSIBLE ROOM BY USING ADVANCED ENCRYPTION STANDARD AND LEAST SIGNIFICANT BIT ALGORITHM

[1]Alaa Jabbar Qasim Al-Maliki

[2]Y V K Sudhakar

[1]M.Sc (Computer Science) Mahatma Gandhi College Affiliated to Acharya Nagarjuna University Guntur,AP, India, neenalaa@gmail.com

[2]M.Tech (CSE) Mahatma Gandhi College Affiliated to Acharya Nagarjuna University Guntur, AP, India, sudakartechcs@yahoo.com

ABSTRACT

There are also a number of works on data hiding in the encrypted domain. The reversible data hiding in encrypted image is investigated in. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain .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. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. 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. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted Images. Experiments show that this method can embed more than 10 times as large payloads for the same image quality as the previous methods .The data extraction and image recovery can be achieved by examining the block smoothness. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.[1]

Key words: *Reversible Data Hiding (RDH),, image encryption, , least significant bits*

1. INTRODUCTION

Reversible data hiding (RDH) is a technique in image Processing area for encryption, by which the original cover can be lossless recovered after the embedded message is extracted. The RDH approach is widely used in medical science, defense field and forensic lab, where there is no degradation of the original content is allowed. Since more research RDH method in recently. In theoretical aspect rate-distortion model for RDH , through which they proved the rate-distortion bounds of RDH for memory less covers and proposed a recursive code construction which, however, does not approach the bound. The recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes the equivalence between data compression and RDH for binary covers. Many RDH techniques have emerged in recent years. Fridrich *et al*[2] constructed a general framework for RDH for method . By first extracting compressible features of original cover and then compressing them lossless, spare space can be saved for embedding auxiliary data. A various RDH method is more popular is based on difference expansion (DE)[3], in which the difference of each pixel group is expanded by various method or technique. Example, multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another reliable strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values. With respective to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to non-readable one. Although there are few RDH techniques in encrypted images have been published yet, there are some promising applications if RDH can be applied to encrypted images. Hwang ET *al.*advocated a reputation-based trust management

Scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. In our system we provide the high quality image to the users. It also provides the more security of the data. The proposed system is reduces the time as well as cost as compared to previous system. [2].

2. LITERATURE SURVEY

2.1 Reversible Data Embedding Using a Difference Expansion
Jun Tian , ieee transactions on circuits and systems for video technology, vol. 13, no. 8, august 2003 . In this paper, we present a novel reversible data embedding method for digital images. We explore the redundancy in digital images to achieve very high embedding capacity, and keep the distortion low.

2.2 On Compressing Encrypted Data
Mark Johnson, *Student Member, IEEE*, Prakash Ishwar, Vinod Prabhakaran, *Student Member, IEEE*
In this paper, we investigate the novelty of reversing the order of these steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security. Although counter-intuitive, we show surprisingly that, through the use of coding with side information principles, this reversal of order is indeed possible in some settings of interest without loss of either optimal coding efficiency or perfect secrecy.

2.3 Expansion Embedding Techniques for Reversible Watermarking
Diljith M. Thodi and Jeffrey J. Rodríguez, *Senior Member, IEEE*
First, we have presented the histogram-shifting technique to remedy the two major drawbacks of Tian's algorithm: the lack of capacity control and undesirable distortion at low embedding capacities. We then described two new reversible watermarking algorithms, combining histogram shifting and difference expansion: the first one using a highly compressible overflow map and the second one using flag bits. A new, reversible, data-embedding technique called prediction-error expansion was then introduced and watermarking algorithms based on the prediction- error expansion technique were presented.

2.4 A Reversible Data Hiding Scheme Based on Block Division Wen-Chung Kuo1, Dong-Jin Jiang1 and Yu-Chih Huang2, Department of Computer Science and Information Engineering,
In this paper, a reversible data hiding scheme based on histogram is proposed. In this proposed scheme, there are two advantages: 1. our proposed scheme are able to improve the fact embedding capacity by using block division method, 2. we use one bit to record the change of the selected minimum point to achieve not only higher data hiding capacity but also the reversible effect.

2.5 Efficient Compression of Encrypted Grayscale Images
wei Liu, Member, IEEE, Wenjun Zeng, Senior Member, IEEE , In this correspondence, we focus on the design and analysis of a practical lossless image codec, where the image data undergoes stream-cipher based encryption before compression .We propose resolution progressive compression for this problem, which has been shown to have much better coding efficiency and less computational complexity than existing approaches.

3. EXISTING SYSTEM

1) In the existing System more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless Recovered after embedded data is extracted while protecting the image content's confidentiality.
2) 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.
3) 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.

4. PROPOSED SYSTEM

1) This method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.
2) This method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.
3) 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.

5. ARCHITECTURE SYSTEM

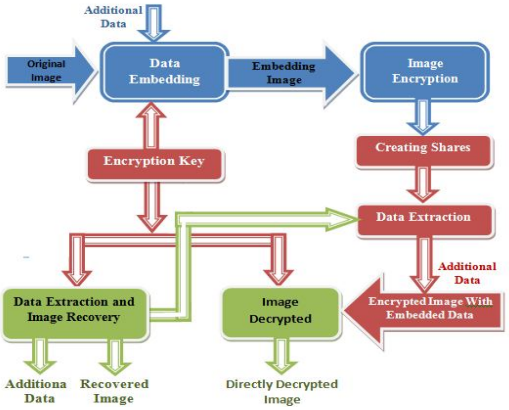

Figure 1 shows the architecture system

6. MODULE DESCRIPTION

6.1 reversible data hiding : Reversible data hiding is very useful for some extremely image such like medical images and military images. In the reversible data hiding schemes, some schemes are good performance at hiding capacity but have a bad stego image quality, some schemes are good stego image quality but have a low hiding capacity. It is difficult to find the balance between the hiding capacity and stego image quality. In this paper, a novel reversible data hiding scheme is proposed. The proposed scheme uses a new embedding method, which is called Even-Odd embedding method, to keep the stego image quality in an acceptable level, and uses the multi-layer embedding to increase the hiding capacity.[4]

6.2 image encryption : This module describes the encryption of image to be transmitted. Here we use visual cryptography algorithm for encrypt the image. So first the image is converting into streams of data array and each data will be encrypted. The shares will be created based on the number of users. For example if 5 users are there means we create five shares. For each share the user can reveal the image but only after five shares he can view the full image. This algorithm not uses the encryption key because if the key is obtained by some unauthorized person then he will reveal the image very easily.

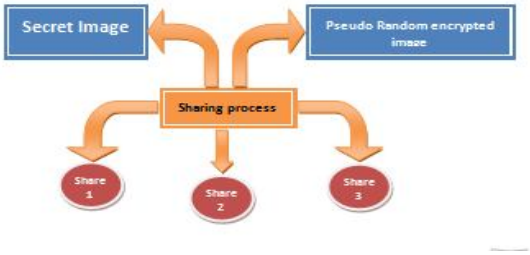

Figure 2 shows the sharing process in system

7. ALGORITHMS USED

7.1 advanced encryption standard (AES): definition

The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector. (Encryption for the US military and other classified communications is handled by separate, secret algorithms.)In January of 1997, a process was initiated by the National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department, to find a more robust replacement for the Data Encryption Standard (DES) and to a lesser degree Triple DES. The specification called for a symmetric algorithm (same key for encryption and decryption) using block encryption (see block cipher) of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next 20 to 30 years. It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques. The entire selection process was fully open to public scrutiny and comment, it being decided that full visibility would ensure the best possible analysis of the designs. In 1998, the NIST selected 15 candidates for the AES, which were then subject to preliminary analysis by the world cryptographic community, including the National Security Agency. On the basis of this, in August 1999, NIST selected five algorithms for more extensive analysis. These were:

- MARS, submitted by a large team from IBM Research
- RC6, submitted by RSA Security

- Rijndael, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- Serpent, submitted by Ross Andersen, Eli Biham and Lars Knudsen
- Two fish, submitted by a large team of researchers including Counterpane's respected cryptographer, Bruce Schneier

Implementations of all of the above were tested extensively in ANSI C and Java languages for speed and reliability in such measures as encryption and decryption speeds, key and algorithm set-up time and resistance to various attacks, both in hardware- and software-centric systems. Once again, detailed analysis was provided by the global cryptographic community (including some teams trying to break their own submissions). the end result was that on october 2, 2000, nist announced that rijndael had been selected as the proposed standard. on december 6, 2001, the secretary of commerce officially approved federal information processing standard (fips) 197, which specifies that all sensitive, unclassified documents will use rijndael as the advanced encryption standard. also see cryptography, data recovery agent (dra)related glossary terms**:** rsa algorithm (rivest-shamir-adleman), data key, greynet (or graynet), spam cocktail (or anti-spam cocktail), finger scanning (fingerprint scanning),munging, insider threat, authentication server, defense in depth, nonrepudiation[5]

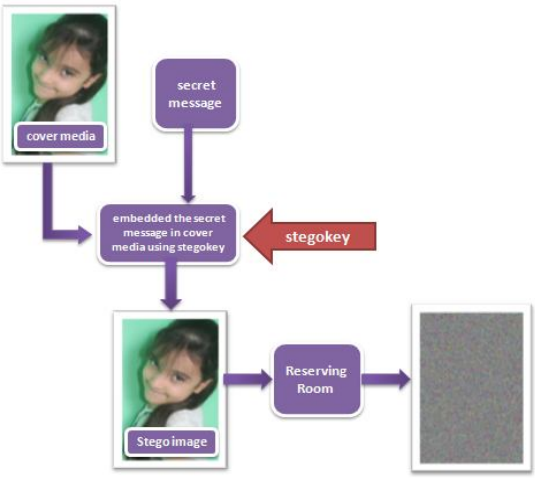

Figure 3 the process of embedding text within the image by using Reserving

7.2 LSB: LEAST SIGNIFICANT BITS

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). Least significant bits are frequently employed in pseudorandom number generators, hash functions and checksums. LSB, in all capitals, can also stand for "Least Significant Byte". The meaning is parallel to the above: it is the byte (or octet) in that position of a multi-byte number which has the least potential value in Steganography a message might be hidden or encrypt within in an image by changing least significant bit to be the message bits then the image

Can be transmitted through network.lsb based Steganography is perhaps the most simple and straight forward approach. In this will only affect each pixel by +\-1, if at all, it is generally assumed with good reason that degradation caused by this embedding process would perceptually transparent. Hence there are number of lsb based Steganography techniques in the passive warden model as it difficult to differentiate cover-image from stegoimages, given the small changes that have been made. There are many methods for steganography; to hide the secret message into the image.LSB is the well known method for data hiding. The approaches for steganography that are based on LSB can be found .The another is PVD Method i.e. pixel-value differencing method divides the cover image into blocks and modifies the pixel difference in each block for data embedding. Gray-level modification Steganography is a technique to map data by modifying the gray level values of the image pixels. It uses the odd and even numbers to map data within an image. [6]

Figure 4 cover image

Figure 5 stego image

8. CONCLUSION

In A novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and

data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. 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 the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. However, the lossy compression method compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation. [7]

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] 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.

Alaa Jabbar Qasim received the B.S. in Computer Science/ information system Department at Al Rafidain University College in (2000)-Iraq; he is doing M.Sc (Computer Science) Mahatma Gandhi College Affiliated to Acharya Nagarjuna University Guntur, AP, and India. He is interesting in the following Fields (Cryptology, Information Security and Information Hiding)