Hiding of Data and Images Using Huffman Coding

V.Parameshwari
Assistant Professor, Department of ECE, Nandha Engineering College, Erode-52, Tamilnadu, India.

V.Logeswari
Assistant Professor, Department of ECE, Nandha Engineering College, Erode-52, Tamilnadu, India.

G.Pradeepkumar
Assistant Professor, Department of ECE, Nandha Engineering College, Erode-52, Tamilnadu, India.

Abstract – Reversible data hiding (RDH) is a technique that embeds secret data into an image in reversible manner. The secret data to be sent is embedded into an image and then transmitted to the receiver. In existing system, the secret data is embedded into an uncompressed image for transmission and LSB technique is used for encrypting an image. In proposed system, any sort of image is taken as input and then converted into JPEG format. Further they are compressed which may increase the efficiency. Here Huffman coding technique is used for image compression. Added to this the data is embedded in an image. Here both secret data and image gets encrypted using AES algorithm and then secret data is embedded into the encrypted image. Finally key is exchanged between sender and receiver through the image. With the help of the key the receiver can be able to retrieve both image and the Secret message. By doing compression before encryption will make the system more efficient. This proposed method is to be considered the patch-level sparse representation when hiding the secret data. A large vacated room can be achieved, and thus the data hider can embed more secret messages in the encrypted image.

Index Terms – Image encryption, reversible data hiding (RDH), Huffman coding.

1. INTRODUCTION

Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the buildup of noise and signal distortion. Image processing techniques involve treating the image as two-dimensional signal and applying standard signal processing techniques to it. Some of the efficient algorithms used in image processing are RSA, AES etc. In some cases techniques like Huffman coding, least significant bits for image encryption process. This paper is concerned about transmitting confidential data by embedding it into an encrypted image. Huffman coding technique is used to compress an image, this technique is mainly used to transmit data in well-organized manner which provides security without any data loss during the process of transmission.

Image of any format is converted to JPEG image and encrypted where the encrypted data is embedded into it. Both embedded and encryption key has sent to receiver. The receiver extracts the data and image with the key.Reversible data hiding (RDH) in images aims to exactly recover both the embedded secret information and the original cover image. It has attracted intensive research interests. Military, medical and legal scenarios are its typical examples, in which even a slight distortion is not tolerable. Many RDH algorithms have already been developed, such as image compression-based, difference expansion-based, histogram shift (HS)-based, image pixel pair based, and dual/multi-image hiding methods. Recently, due to the requirement of privacy protection, the cover owner usually encrypts the original content before transferring it to the data manager. Meanwhile, the data manager may want to embed additional messages into the above have provided promising encrypted domains, they are insufficient for more sensitive military and medical scenarios, where the image content should be not only kept secret strictly, but also be losslessly recovered after data extraction. Therefore, RDH in encrypted images (RDHEIs) is desirable. To this end, many RDHEI schemes have been proposed in past years.

One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the three LSBs of the cover-image with the message bits, which is kind of the pixel-level compressive methods essentially. In[23], the encrypted image is segmented into a number of non overlapped blocks, while each block is divided into two sets. Each block carries one bit by flipping three LSBs of a set for predefined pixels. Hong et al. [24] gave an improved version based on [23]. Specifically, they fully harness the pixels in calculating the smoothness of each block and consider the pixel correlations in the border of neigh- boring blocks. The resulting error rate of extracted-bits is thereby decreased. In [25], the proposed method creates a sparse space to accommodate some additional data by com- pressing the LSBs of the encrypted image. It is hard to squeeze room by only considering three LSBs of the encrypted images.

Reversible data hiding (RDH) in images aims to exactly recover both the embedded secret information and the original cover image. Due to the requirement of privacy protection the cover owner usually encrypts the original content before transferring it to the data manager.

2. RELATED WORK

Weiming Zhang, Biao Chen, and Nenghai Yu proposed a decompression algorithm [2]as the coding scheme for embedding data. Three RDH schemes that use binary feature sequence as covers, i.e., one scheme for substitution scheme for binary images. Nosrati and some other people [3] present the paper Reversible Data Hiding: Principles, Techniques, and Recent Studies. In this primary techniques as the principles of RHD are talked. Pairwise logical computation data hiding technique (PWLC) and Data hiding by template ranking with symmetrical Central pixels(DHTC) technique. In Image processing for transmission there are many threats like data hacking. Hacker will crack the secret data which is to be shared between sender and receiver. This type of transmission used in the field of army military purpose, medical field and all other field which needs secured transmission. Some of the issues faced are under follows. In some cases the data is embedded in the image for secured transmission. The image which is transmitted is not encrypted so that they can be easily hacked by the hacker[4]. Secret data is embedded into the encrypted image. It is easy to find the key for encrypted image hence the image is decrypted and data is extracted[5]. Zhang [6] suggests a novel method for separable reversible data hiding .Here content owner first encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB,a decryption with the encryption key can result in an image similar tothe original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extractedand the original image can be perfectly recovered by exploiting the spatial correlation in natural image. In [7] C. Anuradha and S. Lavanya proposed a secure and authenticated descrete reversible Data hiding in cipher images deals with security and authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received 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 encryption key, can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large. It is also a drawback because if the receiver has any one key as known, and then he can take any one information from the encrypted data. In order to achieve authentication SHA-1 algorithm is being used.

3. PROPOSED MODELLING

In proposed system any type of cover image is taken as input, then it is converted into JPEG image then the image is compressed and converted using Huffman algorithm. Image encryption has to be done here to improve its security. The encryption and embedding are controlled by encryption and embedding keys given by the sender. Reversible data hiding technique is going to be used now sender has his own choice of giving keys to receiver that is it may be both key ,it may be data key(embedding key)alone or it may be encryption key alone. With the help of this key receiver could obtain Image and data if and only if he has both encryption and embedding key. If receiver has only data key he could extract only Secret data. Extraction is done after decrypting the received content. By this way a data is sent to the receiver in a very confidential manner. This is very important in many fields like army, military, airforce etc.

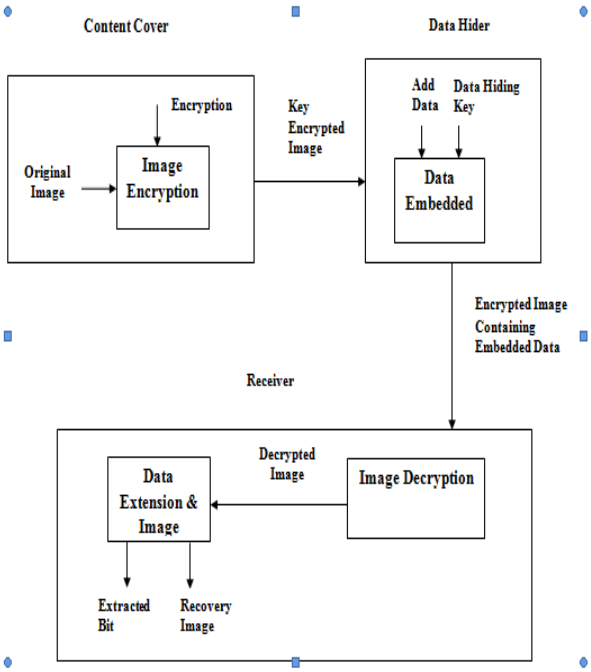

Figure 1 Block diagram of proposed system

A. Huffman coding

Huffman codes can be used to compress information Like WinZip – although WinZip doesn't use the Huffman algorithm JPEGs do use Huffman as part of their compression process.The basic idea is that instead of storing each character in a file as an 8-bit ASCII value, we will instead store the more frequently occurring characters using fewer bits and less frequently occurring characters using more bits. On average this should decrease the file size (usually ½).Un compressing works by reading in the file bit by bit start at the root of the tree If a 0 is read, head left. If a 1 is read, head right When a leaf is reached decode that character and start over again at the root of the tree Thus, we need to save Huffman table information as a header in the compressed file.

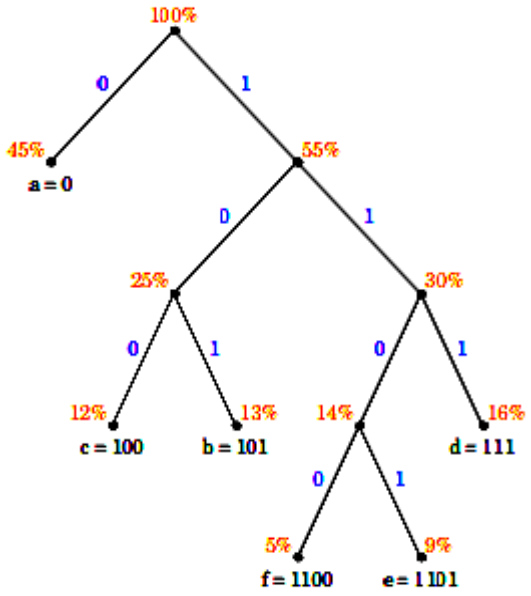

Figure 2 Representation of a binary code as binary tree

Huffman coding is optimal when each input symbol is a known independent and identically distributed random variable having a probability that is and the inverse of a power of two. Prefix codes tend to have inefficiency on small alphabets, where probabilities often fall between these optimal points. The worst case for Huffman coding can happen when the probability of a symbol exceeds 2−1 = 0.5, making the upper limit of inefficiency unbounded. These situations often respond well to a form of blocking called run-length encoding. For a set of symbols with a uniform probability distribution and a number of members which is a power of two, Huffman coding is equivalent to simple binary block encoding, e.g., ASCII coding. This reflects the fact that compression is not possible with such an input. Huffman coding is done with two major steps which are explained as follows.

4. RESULTS AND DISCUSSIONS

Performance Analysis

PSNR is defined as the ratio between maxim power of the signal and power of noise. The signal in this case is the original data, and the noise is the error introduced by compression.

Experimental value of the image Lena and here we calculate the value of PSNR, TIME, here the time is calculated to encrypt the image.

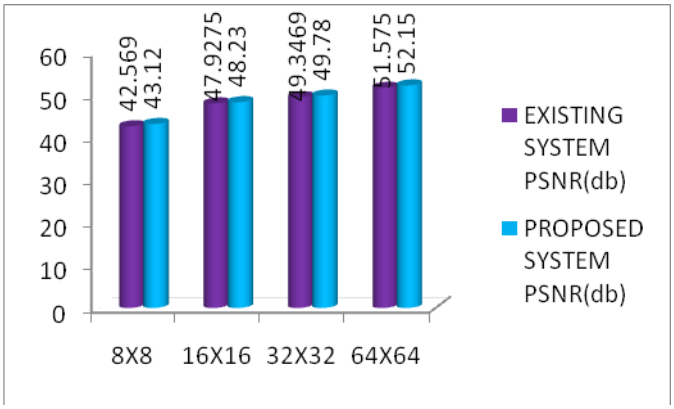

Figure 3 Comparison graph between existing system PSNR and proposed system PSNR

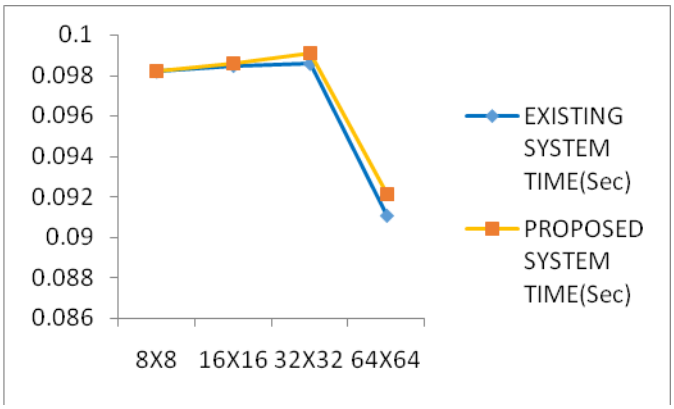

Figure 4 Comparison graph between existing system time and proposed system time

5. CONCLUSION

After comparing various algorithms and techniques for data hiding, the Huffman coding technique has been achieved the highest PSNR for different images. Further they are compressed which has increased the efficiency. The proposed system is to be considered the patch-level sparse representation when hiding the secret data. A large vacated room can be achieved, and thus the data hider can embed more secret messages in the encrypted image.

REFERENCE

[1] M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.
[2] 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.
[3] Nosrati * Ronak Karimi Mehdi Hariri," Reversible Data Hiding:Principles, Techniques, and Recent Studies". World Applied Programming, Vol (2), Issue (5), May 2012. 349-353ISSN: 2222-2510©2011 WAP journal.
[4] Z. Ni, Y. Shi, and N. Ansari et al., "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.
[5] X. Zhang, "Reversible data hiding in encrypted images," IEEE signal process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[6] X. Zhang, "Separable reversible data hiding in encrypted image," IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[7] C. Anuradha and S. Lavanya "A secure and authenticated reversible Data hiding in encrpted images" © 2013, IJARCSSE.
[8] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for JPEG images," in Proc. Inf. Technol. Coding Comput., Las Vegas, NV, USA, Apr. 2001, pp. 223–227
[9] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel dif- ference expansion transform for reversible data embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 456–465, Sep. 2008.
[10] D. Coltuc, "Improved embedding for prediction based reversible watermarking," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873–882, Sep. 2011.
[11] X. Li, B. Ying, and T. 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.
[12] Y. Hu, H. K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1511, Dec. 2008.
[13] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise prediction- error expansion for efficient reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 12, pp. 5010–5021, Dec. 2013.
[14] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906–910, Jun. 2009.
[15] C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," Pattern Recognit., vol. 41, no. 12, pp. 3582–3591, Dec. 2008. \
[16] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, no. 6, pp. 1129–1143, Jun. 2009.
[17] S. L. Lin, C. F. Huang, M. H. Liou, and C. Y. Chen, "Improving histogram-based reversible information hiding by an optimal weight-based prediction scheme," J. Inf. Hiding Multimedia Signal Process., vol. 4, no. 1, pp. 19–33, Jan. 2013.
[18] S. W. Weng, Y. Zhao, R. R. Ni, and J. S. Pan, "Parity-invariability-based reversible watermarking," Electron. Lett., vol. 45, no. 20, pp. 1022–1023, Sep. 2009.
[19] S. Weng, Y. Zhao, J. S. Pan, and R. Ni, "Reversible watermarking based on invariability and adjustment on pixel pairs," IEEE Signal Process. Lett., vol. 15, no. 20, pp. 721–724, Dec. 2008.
[20] C. F. Lee and Y. L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations," J. Telecommun. Syst., vol. 52, no. 4, pp. 2237–2247, 2013.
[21] G. Horng, Y. H. Huang, C. C. Chang, and Y. Liu, "(k, n)-image reversible data hiding," J. Inf. Hiding Multimedia Signal Process., vol. 5, no. 2, pp. 152–164, Apr. 2014.
[22] Y. Wang and K. N. Plataniotis, "An analysis of random projection for changeable and privacy-preserving biometric verification," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 40, no. 5, pp. 1280–1293, Oct. 2010.
[23] A. Dabrowski, E. R. Weippl, and I. Echizen, "Framework based on privacy policy hiding for preventing unauthorized face image processing," in Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC), Manchester, U.K., Oct. 2013, pp. 455–461.
[24] Y. T. Wu and F. Y. Shih, "Genetic algorithm based methodology for breaking the steganalytic systems," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 36, no. 1, pp. 24–31, Feb. 2006.
[25] X. Gao, C. Deng, X. Li, and D. Tao, "Geometric distortion insensitive image watermarking in affine covariant regions," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 40, no. 3, pp. 278–286, May 2010.