A Critical Review: Data Hiding Techniques for Image Compression

[1]Shivani Patel, [2]Prof. Hemant Amhia

[1]M.Tech Scholar, [2]Assistant Professor
JEC, Jabalpur

Abstract: **Information security has always been a major concern. As one of the ways to solve the security problem, data hiding technology embeds the secret data imperceptibly into the cover media by slightly modifying some of the cover elements. Traditional data hiding techniques usually introduce irreversible distortion in the cover media which cannot be recovered after secret data extraction. However, the distortion may be not allowed in the medical, military and legal fields. To overcome this problem, paper discusses reversible data hiding in JPEG compressed image as a new solution where both secret data and the original cover media can be extracted and recovered without any distortion. Moreover, data hiding techniques can be applied to other aspects such as embedding patient's information into medical images and embedding geographic information into remote sensing satellite images. MATLAB standard image of lena will be used for the testing of the proposed work in near future as the same taken by base works the testing lena image of 512x512 size and the data hidden is of 1 Kb. expected PSNR**

Keywords: **DWT: Discrete Wavelet Transform, SVD: Singular Value Decomposition, PSNR: Peak Signal to Noise Ratio, MSE: Mean Square Error.**

I. INTRODUCTION

Steganography[4] use data hiding instead of data modification which does not attract intruders to even try to decode the data. Figure 1 below shows the Steganography method.

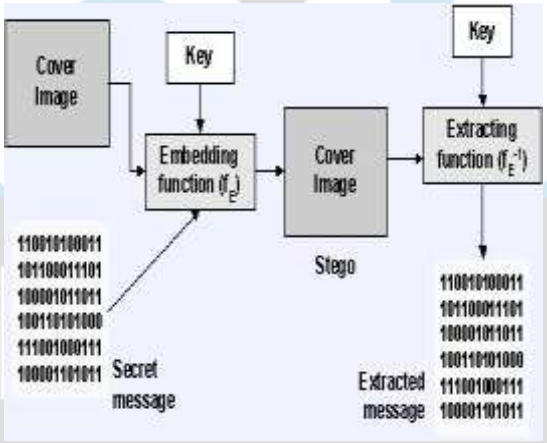

Fig.1 Data Hiding using Steganography

Steganography is the embedding of messages within an innocuous cover work in a way which cannot be detected by anyone without access to the appropriate steganography key. A popular attack in Steganography[4] is the compression. Figure 2 below shows the image compression. In compression lots of information gets loss and the recovered pixels does remains exact same as it was in its original image and it may cause loss of hidden data in original image.

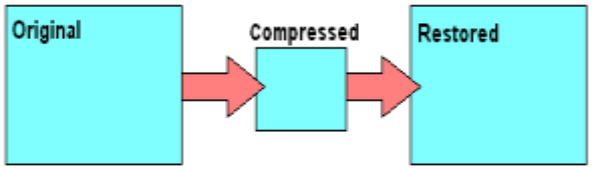

Fig. 2 Image Compression

Hence stenographic methods fails when image compression used and if we did not use image compression lots of data need to be transmit which cause communication delay and bandwidth loss.

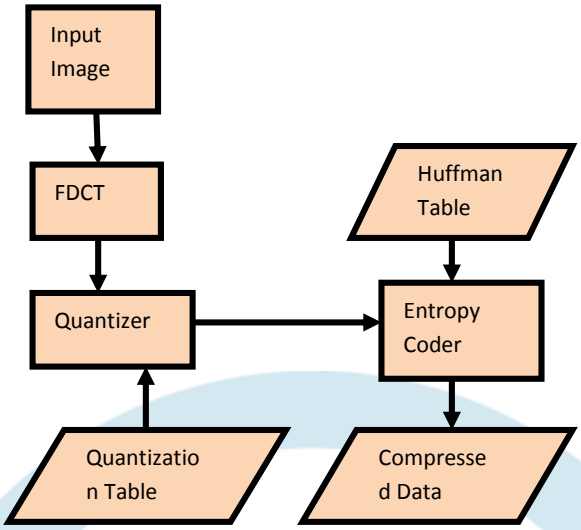

Fig. 3 The block diagram of the JPEG encoder

JPEG compression procedure: In this section, a brief introduction to the JPEG concept and the JPEG compression process are given[5]. JPEG is a common lossy compression method for digital images. The JPEG standard consists of two types of compression methods, i.e., DCT-based methods and prediction-based methods by Wallace (1991).The former are designed for lossy compression, while the latter are designed for lossless compression. JPEG features a simple lossy mode known as the Baseline method which is a subset of the other DCT-based modes of operation. The Baseline method has been the most widely used JPEG method so far, thus this paper focuses on the Baseline method of Image Encoding. Fig. 3 shows the main steps of the Baseline method. An input image is first divided into 8 × 8 non-overlapping blocks, and then each block is applied by the forward DCT (FDCT) to get a set of 64 DCT coefficients. Mathematical definitions of 8 × 8 FDCT and 8 × 8 inverse DCT (IDCT) are as follows:

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)\cos\frac{(2x+1)u\pi}{16}\ \cos\frac{(2y+1)v\pi}{16}\right]$$

$$f(x,y) = \frac{1}{4}C(u)C(v)\left[\sum_{u=0}^{7}\sum_{v=0}^{7} F(u,v)\cos\frac{(2x+1)u\pi}{16}\ \cos\frac{(2y+1)v\pi}{16}\right]$$

$$\text{where } c(u) = \begin{cases} \frac{1}{\sqrt{2}} & u = 0 \\ 1 & \text{otherwise} \end{cases}$$

To compress the image data, these coefficients are then quantized by using a quantization table with 64 entries. The standard quantization table is shown in Fig. 4. The quantized coefficients are all integers which are obtained by dividing each DCT coefficient by its corresponding value in the quantization table and rounding to the nearest integer as follows:

$$D(u,v) = \text{integer Round}\left(\frac{F(u,v)}{Qu,v)}\right)$$

where F(u, v) means the original DCT coefficient, Q(u, v) means the corresponding value in the quantization table and D(u, v) means the quantized DCT coefficient. Because of the rounding loss, the quantization step is not lossless. The final data stored in the JPEG file are the quantized DCT coefficients, which are entropy coded and saved in the entropy-coded segment of the JPEG file. The quantization table is stored in the DQT (define quantization table) segment. In this paper, our experiment is done with the JPEG library "Libjpeg"

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 22 & 29 & 68 & 109 & 103 & 77 \\ 24 & 35 & 37 & 56 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 121 & 120 & 120 & 101 \\ 72 & 92 & 95 & 98 & 100 & 103 & 103 & 99 \end{bmatrix}$$

Fig. 4 JPEG standard quantization table.

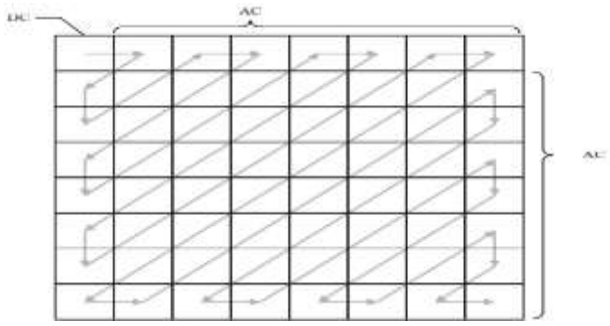

Fig. 5 Zigzag sequence

The quantization table in Libjpeg is controlled by quality factor QF which is an integer in the interval [1,100]. Libjpeg adopts the following transformation to get the scale factor to form a new quantization table:

$$\text{Scale Factor} = \begin{cases} \frac{5000}{\text{QF}} & \text{QF} < 50 \\ 200 - 2\text{QF} & \text{otherwise} \end{cases}$$

Then it multiplies every entry of the standard quantization table by ScaleFactor/100 and then rounds the resulting value to its nearest integer. If the result is smaller than 1, then it is set to 1.

$$Q_{new}(u,v) = \max\left(\text{IntegerRound}\left(\frac{Q_{Standard}(u,v).\,\text{ScaleFactor}}{100}\right), 1\right)$$

From Eqs.(4) and (5), we can see that when the image quality factor QF equals 50, the standard quantization table is used. The final step is the lossless step called entropy coding. The quantized coefficients are first scanned in the zigzag manner as shown in Fig. 5. For natural images, there are a lot of consecutive zeros in high-frequency portion, which helps to further compress the image using entropy coding. Thus, AC coefficients can be encoded by Zero Run Length Coding (ZRLC). DC coefficient corresponds to the lowest frequency in an 8 × 8 block, which is the average value over the 64 pixels. Usually there is a very close correlation between the DCT coefficients of adjacent blocks, thus the encoding ofthe quantized DC coefficient is performed on the difference between the quantized DC coefficients of the two consecutive blocks.

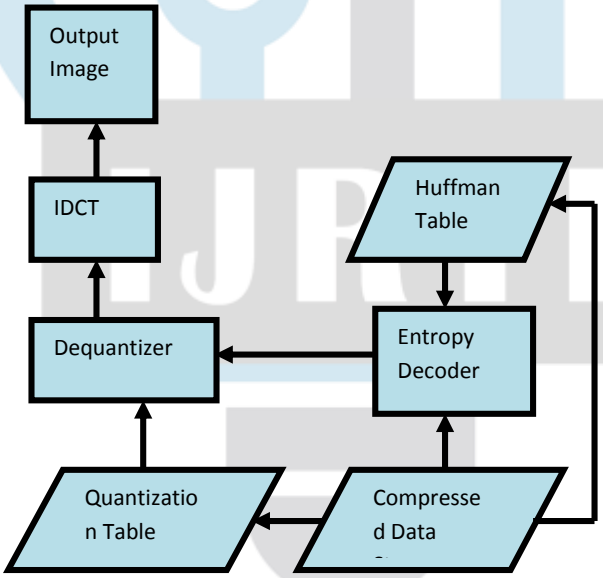

Fig. 6 JPEG decoding process

Finally, the intermediate sequence of symbols is converted to a data stream by Huffman coding. The JPEG decoding process shown in Fig. 6 is the inverse process of JPEG encoding. The decoding process mainly consists of three steps, i.e., Entropy decoding, dequantization and IDCT. The decoder reads the quantization table and the quantized DCT coefficients from the DQT segment and entropy-coded segment, respectively. The decoder then multiplies the quantized DCT coefficients by corresponding elements in the quantization table and applies inverse DCT to the results to obtain uncompressed image

II. LITERATURE SURVEY

Most of the existing data hiding techniques focus on the spatial domain and transform domains, while only a few pay attention to compressed domains. On the Internet, images in compressed format have become very popular for the reason that they can save a lot of storage space and improve the transmission efficiency. JPEG format is one of the most popular formats and widely used on

various platforms. Upham (1997) [14] first developed a famous hiding tool for JPEG images named Jpeg-Jpeg, where the secret data are embedded into the least significant bits (LSB) of the quantized DCT coefficients whose values are not 0, 1 or −1. Westfeld (2001)[16] developed a so called F5 algorithm which implements matrix encoding to improve the embedding efficiency. In addition, F5 also employs permutative straddling to uniformly spread out the changes over the whole steganogram. Both methods mentioned above are irreversible with a low capacity.

In the same year, Fridrich et al. (2001)[8] presented for the first time an invertible watermarking method for authentication of digital images in the JPEG domain, where they modified the quantization matrix to enable lossless embedding of one bit per DCT coefficient. Fridrich et al. (2002)[9] proposed a new idea to losslessly compress the LSB plane of some selected JPEG mode coefficients in order to make space for reversible data embedding. Later, Chang et al. (2002)[19] presented a reversible hiding scheme to modify the quantization table and hide the secret data in the cover image based on the mid-frequency quantized DCT coefficients.

Iwata et al. (2004)[11] proposed a hiding scheme by modifying the boundaries between zero and non-zero quantized DCT coefficients in each block. However, it is irreversible with a low capacity. Inspired by Iwata et al.'s scheme, Chang et al. (2007) proposed a lossless steganography scheme to hide secret data in the quantized DCT coefficients of each block in JPEG images.

In the same year, Xuan et al. (2007)[17] proposed a scheme to shift the quantized DCT coefficient histogram and then embed data based on histogram pairs. Later, Sakai et al. (2008)[13] improved Xuan et al.'s scheme and yielded better image quality by judging whether a block is suitable for embedding data or not. Almohammad et al. (2009) [6] extended the method of Chang et al.(2002) [19] by using an optimized 16 × 16 quantization table and improved the stego image quality and the embedding capacity. Later, Cheng and Yoo (2009)[7] proposed a reversible scheme which is similar to Iwata's scheme and the scheme of Chang et al. (2007) [20]and performed multi-level embedding to reach a higher capacity. Zhang et al. (2010)[18] proposed a reversible data hiding method to carry the watermark for JPEG image authentication.

Among various data hiding techniques, the reversible ones for the JPEG domain are still only a few and there is a huge margin for improvement in both the stego image quality and the capacity. The method of Fridrich et al. (2002)[9] divided some elements of the quantization table by a factor; at the same time, the corresponding quantized DCT coefficients were simply multiplied by the same factor to make space for embedding. Lin and Chan (2010) [12] proposed an invertible secret image sharing with a steganography scheme. The secret pixels are firstly transformed into k-ary notational numbers, then encrypted into shared data, and finally shared along with the information data based on the (t,n)-threshold sharing scheme with a modulo operation.

Xiaozhu Xie et al [1] use scheme of reversible data hiding in encrypted image (RDH-EI) with high embedding capacity is proposed in this paper. First, cover image is transformed to the quantized discrete cosine transform (DCT) coefficients, which are reformed and encrypted to generate the encrypted image. Then the secret message is embedded into the encrypted image in the location of zero alternating current (ac) coefficients to generate the marked encrypted image. The JPEG image can be recovered by using the encryption key

The secret message can be extracted using the embedding key. The experimental results showed that the proposed scheme can obtain a high embedding ratio while ensuring that the recovered image will have good quality. Lu ıs F. R. Lucas et al [2] use highly efficient method for lossless compression of volumetric sets of medical images, such as CTs or MRIs. The proposed method, referred to as 3D-MRP, is based on the principle of minimum rate predictors (MRP), which is one of the state-of-the-art lossless compression technologies, presented in the data compression literature. The main features of the proposed method include the use of 3D predictors, 3D-block partitioning and classification, volume-based optimisation and support for 16 bit-depth images. Experimental results demonstrate the efficiency of the 3D-MRP algorithm for the compression of volumetric sets of medical images, achieving gains above 15% and 12% for 8 bit and 16 bit-depth contents, respectively, when compared to JPEG-LS, JPEG2000, CALIC, HEVC, as well as other proposals based on MRP algorithm.

Parameter for the valuation of the work are PSNR and MSE, Mean square error is the error estimation between two image and PSNR is the error amount in the image, MSE can be computer as below

$$MSE = \frac{1}{rc}\sum_{i==1}^{RW}\sum_{j=1}^{CL}(x_{ij} - y_{ij})^2$$

.

TABLE 1: AVAILABLE WORK REVIEW

Paper	Author	Method	Pros / Cons
Reversible Data Hiding in Encrypted Images Using Reformed JPEG Compression	Xiaozhu Xie, Chin-Chen Chang	In this method the Reversible data hiding in encrypted images (RDH-EI), cover image is transformed to the quantized discrete cosine transform (DCT) coefficients, which are reformed and encrypted to generate the encrypted image. Then the secret Message is embedded into the encrypted image in the location of zero alternating current (ac).	Pros- high PSNR and data embedding rate is also high. Cons- their code embed the data at AC components only which may leads to low data density.
A Reversible JPEG-to-JPEG Data Hiding Technique	Ziqiang Cheng, Kee-Young Yoo	Novel reversible JPEG-to-JPEG data hiding technique. It uses a compressed JPEG image as a cover and embeds secret data into selected tuples in 8 × 8 quantized DCT coefficient blocks to generate a JPEG stego image finally.	Pro-Hiding in selected tuples leads High PSNR Cons- The overall less data get hides because of selected AC or DC components
Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3	Abdelhamid Awad Attaby, Mona F.M. Mursi Ahmed, Abdelwahab K. Alsammak	DCT-M3, uses modulus 3 of the difference between two DCT coefficients to embed two bits of the compressed form of the secret message. This algorithm reduces significantly the number of changes in the cover image	Pro- modulus need less bits hence more hiding possible Cons- need to compute modules at transmitter and receiver end
Lossless Compression of Medical Images Using 3D Predictors	Luıs F. R. Lucas, Nuno M. M. Rodrigues, Luis A. da Silva Cruz and Sergio M. M. de Faria	This method, referred to as 3D-MRP, is based on the principle of minimum rate predictors (MRP), which is one of the state-of-the-art lossless compression technologies	Pros- use of 3D predictors, 3D-block octree partitioning and classification, volume-based optimisation and support for 16 bit-depth images. Cons- Highly time consuming as 3D-MRP is a complex algorithm.

Where ‘r’ is the number of rows in the image ‘c’ is the columns in the image x is input image before data hiding, y is the output image after data hiding PSNR can be computed as

$$PSNR = 20log_{10}\left(\frac{256^2}{MSE}\right)$$

Propose work in near future will work expected to have better PSNR and low MSE as compare to available work. With modified data hiding strategy in DCT Compressed image.

IV.CONCLUSION

The problem the JPEG algorithm is designed to solve high PSNR in Steganography and a more efficient means of representing digital images. The solution provided by the JPEG algorithm is extremely effective and widely adapted everywhere. Image Compression is highly sophisticated and closely tied with mathematical operations. The embedding strategy and sequence are optimized in order to get a better stego image have been discussed in the paper and a comparative analysis of available work with pro’s and con’s has been discussed. The procedure of image compression also been discussed in the paper. Among all the papers chosen for comparison, Xiaozhu Xie et al [1] work on reversible data hiding method in compressed JPEG image. In this paper, AC components are used which allows more data to hide and because of this only small changes happens in the original image. In near future we will implement the work with proposed methodology on MATLAB. Excepted PSNR is more than the discussed literature work.

Reference

[1] Xiaozhu Xie, Chin-Chen Chang, Reversible Data Hiding in Encrypted Images Using Reformed JPEG Compression, Natural Science Foundation of P. R. China under Grant 61503316, Natural Science Foundation of Fujian Province under Grant 2016J01326., IEEE 2017
[2] Ziqiang Cheng, Kee-Young Yoo, A Reversible JPEG-to-JPEG Data Hiding Technique, 2009 Fourth International Conference on Innovative Computing, Information and Control, 978-0-7695-3873-0/2017 IEEE
[3] Abdelhamid Awad Attaby, Mona F.M. Mursi Ahmed, Abdelwahab K. Alsammak, Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3, Ain Shams Engineering Journal, ScienceDirect, 10.1016/j.asej.2017.02.003, 2017
[4]Lu´ıs F. R. Lucas, Nuno M. M. Rodrigues, Luis A. da Silva Cruz and S´ergio M. M. de Faria, Lossless Compression of Medical Images Using 3D Predictors, DOI 10.1109/TMI.2017.2714640, IEEE, Transactions on Medical Imaging
[5] Paul T. Chiou, Yu Sun, and G. S. Young A Complexity Analysis of the JPEG Image Compression Algorithm, 978-1-5386-3007-5/17/2017 IEEE
[6]Almohammad, A., Ghinea, G., Hierons, R.M., 2009. JPEG steganography: a performance evaluation of quantization tables. In: Proceedings of IEEE International Conference on Advanced Information Networking and Applications, Bradford, United Kingdom, pp. 471–478.
[7]Cheng, Z., Yoo, K.Y., 2009. A reversible JPEG-to-JPEG data hiding technique. In: Proceedings of 2009 Fourth International Conference on Innovative Computing,Information and Control, Kaohsiung, Taiwan, pp. 635–638.
[8]Fridrich, J., Goljan, M., Du, R., 2001. Invertible authentication watermark for JPEG images. In: Proceedings of IEEE International Conference on Information Technology:Coding and Computing, Las Vegas, NV, USA, pp. 223–227.
[9]Fridrich, J., Goljan, M., Du, R., 2002. Lossless data embedding for all image formats. In: Proceedings of SPIE, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV, vol. 4675, San Jose, CA, pp. 572–583.
[10]Huang, J., Shi, Y.Q., Shi, Y., 2000. Embedding image watermarks in DC components. IEEE Transactions on Circuits and Systems for Video Technology 10 (6),974–979.
[11]Iwata, M., Miyake, K., Shiozaki, A., 2004. Digital steganography utilizing features of JPEG images. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences E87-A (4), 929–936.
[12]Lin, P., Chan, C., 2010. Invertible secret image sharing with steganography. Pattern Recognition Letters 31 (13), 1887–1893.
[13]Sakai, H., Kuribayashi, M., Morii, M., 2008. Adaptive reversible data hiding for JPEG images. In: Proceedings of International Symposium on Information Theory and its Applications, Auckland, New Zealand, pp. 1–6.
[14]Upham, D., 1997. JPEG-JSteg. http://www.funet.fi/pub/crypt/steganography/jpegjsteg- v4.diff.gz
[15]Wallace, G.K., 1991. The JPEG still picture compression standard. Communications of the ACM 34 (4), 30–44.
[16]Westfeld, A., 2001. F5-a steganographic algorithm: high capacity despite better steganalysis. In: Proceedings of the 4th International Workshop on Information Hiding, Pittsburgh, PA, USA, pp. 289–302.
[17]Xuan, G.R., Shi, Y.Q., Ni, Z.C., Chai, P.Q., Cui, X., Tong, X.F., 2007. Reversible data hiding for JPEG images based on histogram pairs. In: Proceedings of International
Conference on Image Analysis and Recognition, Montreal, Canada, pp. 715–727.
[18]Zhang, X., Wang, S., Qian, Z., Feng, G., 2010. Reversible fragile watermarking for locating tampered blocks in JPEG images. Signal Processing 90 (12), 3026–3036.
[19]Chang, C.C., Chen, T.S., Chung, L.Z., 2002. A steganographic method based upon JPEG and quantization table modification. Information Sciences 141 (1–2), 123–138.
[20]Chang, C.C., Lin, C.C., Tseng, C.S., Tai, W.L., "Reversible hiding in DCT-based compressed images". Information Sciences, vol 177 (13), 2007, pp 2768–2786.