JPEG DECOMPRESSION USING BAYESIAN MAP APPROACH WITH SECURITY

[1]SHAIK KARISHMA, [2]Mrs. K. JHANSI RANI

[1]PG Scholar, Dept. Of E.C.E, Jawaharlal Nehru technological university Kakinada, India
[2]Assistant professor, Jawaharlal Nehru technological university Kakinada, India

Abstract: JPEG decompression can be considered as a image reconstruction problem. Standard decompression of JPEG images produces disturbing checkboard pattern and also artifacts along edges. Such problems can be reduced by formulating decompression as an image reconstruction problem using Bayesian maximum a posteriori probability by iterative optimization algorithms. In this type of problem, the prior knowledge about an image is usually given by L1 norm of learned frame prior. Solution of the problem can be achieved very efficiently using alternating direction method of multipliers as iterative optimization algorithm. The proposed robust method of using Bayesian approach on transform matrix compression algorithm restores images very efficiently even for small image size without disturbing JPEG artifacts. In addition to this, for security an algorithm is presented for lossless image encryption using a private key, with variable bit wise rotation image encryption. This is resistance to any statistical related attacks and also fast and efficient for large amount of data. The quality of reconstruction by this approach is shown both visually and interms of SNR.

Keywords: ADMM, artifacts, bayesian MAP , image processing, JPEG.

I.INTRODUCTION

The standard way to store image data is by compression. Image compression can be lossy or lossless. The lossy compression using JPEG standard [1] has become a standard way to store image data. It is based on the quantization of discrete cosine transform (DCT) coefficients. The compression process results loss of information which is artifacts along strong edges and also visually disturbing checkboard pattern. So the JPEG decompression is considered as image reconstruction problem, since the adoption of the JPEG standard in 1992, the image processing community has worked in order to find the efficient methods fo r restoring the original data. Many JPEG decompression methods, from simple filters to more elaborate methods based on more rigorous statistical formulations for suppressing the checkboard pattern and smoothing along strong edges are used. The latter uses the maximum a posterior probability (MAP) principle as an approximation solution. The JPEG restoration, the log-likelihood is quantization constraint set (QCS), which is defined as the interval of DCT coefficients, rounding of which stored as integer coefficients in JPEG file [2]. The alternative is to approximate this QCS by a multivariate Gaussian function which makes optimization simplified and also convergence is speeded up [7]. Compared to QCS the Gaussian approximation of QCS, resulting function has no constraints thus makes optimization of the posterior probability simplified and speeds up convergence [6]. Bayesian approach with learned priors found its use in many image processing compressed sensing and machine learning applications. The difficulty we encounter in this is non smooth functions resulted in this are not easy to optimize by standard methods. This problem made spreading of various first order techniques for optimization of non smooth functions [10], these are fast and simple to implement. The most popular one is alternating direction method of multipliers (ADMM) [11]. It is also known as split-Bregman method, and the accelerated Arrow-Hurwicz algorithm .

The Gaussian approximation of quantization noise used in this gives efficient improved results, it has various advantages. The convergence is improved due to strong convex of the likelihood. It also improves reconstruction quality both visually and in terms of signal to noise ratio (SNR). Application of ADMM on the combination of Gaussian approximation of QCS is used based on our experience with ADMM in other problems. ADMM has asymptotical convergence properties, the behaviour of this is concentrated mainly for small number of iterations, which are relevant in most of the practical applications, this justifies the use of ADMM instead of accelerated primal-dual methods which convergence is improved by using strong convexity of the likelihood function. ADMM is competitive and sometimes even faster than for [13], this makes MAP based iterative methods practical as non-iterative methods.

The quality of reconstruction depends on mainly the choice of image prior probability distribution which is represented by the regularization function. Early many smooth priors are used like Huber function of spatial gradient [7] or quadratic function of gradient [2]. Later methods incorporated non differentiable sparse priors that provided state of art results for various image reconstruction problems [8] which includes the total variation, field of experts, total generalized variation(TGV), non local means, achieving good results at the cost of longer run times.

The total variation based JPEG decompression [3], uses the total variation as a regularization term and solving minimization problem by using primal dual algorithm. It is effective in reducing the noise without oversmoothing sharp boundaries but results shows block artifacts.

Adaptive non local means filter for image deblocking [9]. Non local means filter is anon linear edge preserving smoothing filter, and it can smooth blocking artifacts and preserve the edge details simultaneously. In this filter can be applied to image block and modify its pixel as the weighted sum of its neighbourhood pixels, whose weighted parameter are determined by similarity of image block neighbourhoods.

Later total generalized variation (TGV) proposed by same author [4] for variational image decompression, reconstruction and also zooming. The TGV functional generates total variation (TV) function by using higher order smoothness information. This avoids staircasing effect but it doesn’t favour for natural images.

This can be done by using learned frame priors. They are self dual, efficient to compute and they preserve norm.

Generally these are imposed when there is a need to reconstruct and stability of the reconstruction is an issue. Since these priors doesn't require inversion of matrices they seem to be a natural choice. The security is added by using key number while transmitting and receiving .

Numerous variations of using XOR operation in encypted algorithms is founded, where bitwise XOR is combined with various operations and produces effective algorithms for for encrypting images. For example the well known AES method, despite the effectiveness of AES in encrypting different types of data, specific requirements of some multimedia presents challenges which limited AES effectiveness in encrypting those types of multimedia data. This new approach of employing circular shifting and XOR operations shows lossless image encryption.

II. PROPOSED METHOD

In this approach, the decompression is based on Bayesian MAP. In Bayesian MAP, the posteriori probability of possible observations is estimated and then chooses highest probability image. According to this Bayesian, this posterior probability of possible solutions is proportional to the product of likelihood which is the error occurred in the compression process, and prior probability approximation. In this, instead of maximizing the probability, the negative log probability is minimized which becomes the product this two as sum of negative log likelihood and a regularization function.

We present this approach with DCT transform matrix algorithm which gives highly compressed image over fft based DCT. In this we are using Bayesian MAP for small size inputs. The DCT transform matrix is more efficient for small size inputs than fft based DCT. As a result by using this new approach, the Bayesian MAP gives efficient reconstruction even for small image size. This method is more efficient for small square inputs, as a result for small size images also the Bayesian MAP gives efficient reconstruction of image over other regularization based methods. The improved image reconstruction is shown in terms of SNR. Thus this new approach is robust even for small image size.

The JPEG compression/decompression process is described by a sequence of operators

$$y = C^{-1} Q^{-1} [QCx] \quad (1)$$

where x and y are original and decompressed images respectively .The linear operators are Q and C. The Q is quantization operator and C is DCT operator. x and y are imaged as vectors, and the operators Q and C are matrices. C is block diagonal matrix obtained by square matrices of DCT.Q is diagonal matrix obtained by element wise operation of quantization coefficients by using quantization table which is stored in each JPEG file which means for 64 values for 8*8 blocks. The symmetric encryption used is not only for data protection but also for user authentication. Generally there are three types in encryption. The secret key (SKC) called as symmetric, public key (PKC) called as asymmetric, and hash functions, which is a one way method. Symmetric key encryption is used which gives high security, fast and efficient for large data. It is necessary while communicating over any untrusted medium, particularly the internet. For decompression of JPEG using Bayesian , first image compression include the block wise DCT by transform matrix algorithm and quantization of DCT coefficients, the symmetric encryption is used after compression. It employs bitwise rotation and XOR operations. This method gives lossless encryption of image using a given key. First the image is converted into stream of bytes and it is grouped into different size of blocks. The image is partitioned into set of blocks by given secret key. The block sizes are determined by key, it is obtained by considering half byte of the given key. The given key also determines the number of shifts in each block. The blocks are usually shifted by b bits, here b is dependent on the size of block, the size of block came from the given key only. For block of size B bytes, it is shifted as

$$b = (B \text{ modulo } 4) + 1 \text{ bits}$$

The bitwise rotation is done and the vacant bit positions are filled by shifted out bits. Thus the shifted image is taken and XOR operation is performed with the given key. The decryption is done by inverting the encryption algorithm without data loss. In decryption the sets of bytes are grouped with same size as in encryption process. However, it is done in opposite direction. Thus this new algorithm comes from performing key dependent encryption at bit level. The number of bits shifted and block sizes are key dependent. Changing one or more bits in key changes the block sizes and number of bits shifted. So, large number of possible keys makes brute force attack impossible. Decompression is done using Bayesian approach thus the original image is retrieved efficiently with improve security. The Bayesian decompression is discussed below.

For given observation y, the probability distribution of possible solutions p(y/x) and a prior probability p(x). The bayesian MAP maximizes the posterior probability

$$p(x/y) \sim p(y/x)p(x) \quad (2)$$

where from eq(2), P(x/y) the posterior probability, p(y/x) the likelihood probability, and p(x) is the prior probability. The prior used is learned frame prior which is obtained from the input image that is patches collected from input database [15]. This prior probability is represented by using regularization function. The optimum observation is estimated which is the likelihood probability by maximizing the posterior probability so that the estimated image is close to the original image. It is done by taking distribution of Gaussian, as the quantization is approximated as Gaussian. Joint pdf of Gaussian of possible observations gives product of two functions, which involves negative log likelihood and prior probability which is represented by regularization function. It becomes sum of log likelihood function which is the noise introduced during compression and regularization function eq(4) The sum of two functions is shown which is optimized by ADMM iterative algorithm.

For obtaining this optimized image using Bayesian MAP , it is done by ADMM algorithm as minimization of the two functions requires the iterative optimization algorithm which minimizes sum of two functions and obtains the optimized image. The sum of two log likelihood function and regularization function in Bayesian MAP is minimized by this ADMM algorithm eq(3).

$$\min_{x} f(x) + g(Gx) \quad (3)$$

The MAP solution for this model is a covex problem.

$$\arg\min_{x} \frac{1}{2\sigma_q^2}||\tilde{y} - QCx||^2 + \tau||\emptyset^T x|| \quad (4)$$

$\tilde{y}$ from eq(4) is the quantization coefficients stored in JPEG format. $\tilde{y}$ = QCy. As quantization error is taken as Gaussian approximation. The Gaussian approximation function with variance σ_q^2 is taken as 12, Where variance is unit quantization noise.

$$QCy = QCx + e, \quad e \sim N(0.I\sigma_q^2) \quad (5)$$

Where eq(6) τ is regularization operator which is used from image data base, thus to best fit observation to original image for full convergence. The regularization function is added to obtain the optimized image, as it minimizes the sum of absolute differences between estimated and target image. The regularization used is L1 to obtain optimized image using ADMM algorithm. The scalar parameter τ can be estimated from training data by the distribution fitted as

$$p(x) \; \alpha \; \tau^N e^{-\tau|\emptyset^T x|} \quad (6)$$

Where the maximization of p(x) is done over all x satisfying the interval -0.5 < QCy - QCx ≤ 0.5, the quantization is taken uniform in this interval. N eq(7) is dimension of x. The maximum likelihood is obtained by setting derivative of above eq(6) distribution to 0, which gives the scalar parameter as

Parameter	Bayesian approach on transform matrix method
PSNR	27.50
MSE	7.22
NMSE	0.001

$$\tau = N/|\emptyset^T x| \quad (7)$$

III. RESULTS AND DISCUSSION

The proposed system is coded, implemented in the Matlab environment and the results are presented as follows. For the original image shown in fig1, the symmetric encryption authentication is used as shown in fig(2). Decompression done by Bayesian approach for the quantization of transform matrix DCT coefficients is shown in fig(3), and its reconstruction can be observed in terms of SNR in the table shown(1). The new approach of using transform matrix algorithm with bayesian MAP for decompression improves SNR even for small image size.

Figure: original image

Figure 2: encrypted image

Figure 3: Retrieved Decompressed image

TABLE.1:

IV. CONCLUSION

The fast solution of this transform matrix algorithm of compression and JPEG decompression based on MAP formulation with prior information by ADMM has been presented which is robust even for small image size and addition of the fast and efficient method of bit level symmetric encryption by using bitwise rotation of variable numbers of bits on blocks of different sizes improves high security. In this the Bayesian decompression approach for DCT transform matrix compression algorithm shows that the proposed approach is robust even for small image size. The combination of Gaussian approximation with QCS and the priors used for image decompression also improves SNR, this counter intuitive fact probably results from the partial inadequancy of priors preferring smooth functions in our situation, where high frequencies are damages by JPEG compression Gaussian approximation favors solutions closer to original JPEG decompression, which prevents the algorithm to make result too smooth, as a result the reconstruction is improved and shown in terms of SNR. It can be extended to resolution enhancement of compressed videos.

REFERENCES

[1] ''JPEG file interchange format ,'' Ecma int., Geneva, Switzerland, Tech. Rep ECMA TR/98,2009.

[2] Y. Yang, N. P. Galatsanos, and A. K. Katsaggelos, "Projection-based spatially adaptive reconstruction of block-transform compressed images," IEEE Trans. Image Process., vol. 4, no. 7, pp. 896–908, Jul. 1995.

[3] K. Bredies and M. Holler, "A total variation–based jpeg decompression model," SIAM J. Imag. Sci., vol. 5, no. 1, pp. 366–393, 2012.

[4] K. Bredies and M. Holler, "A TGV-based framework for variational image decompression, zooming, and reconstruction. Part I: Analytics," SIAM J. Imag. Sci., vol. 8, no. 4, pp. 2814–2850, 2015.

[5] M. Sorel and M. Bartos, "Efficient JPEG decompression by the alternating direction method of multipliers," in Proc. Int. Conf. Pattern Recognit., Dec. 2016.

[6] M. A. Robertson and R. L. Stevenson, "DCT quantization noise in compressed images," IEEE Trans. Circuits Syst. Video Technol., vol. 15, no. 1, pp. 27–38, Jan. 2005.

[7] R. L. Stevenson, "Reduction of coding artifacts in transform image coding," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), vol. 5. Apr. 1993, pp. 401–404.

[8] S. Mallat, A Wavelet Tour of Signal Processing: The Sparse Way, 3rd ed.San Diego, CA, USA: Academic, 2008.

[9] C. Wang, J. Zhou, and S. Liu, "Adaptive non-local means filter for image deblocking," Signal Process., Image Commun., vol. 28, no. 5, pp. 522–530, 2013.

[10] J.-F. Cai, S. Osher, and Z. Shen, "Split Bregman methods and framebased image restoration," Multiscale Model. Simul., vol. 8, no. 2, pp. 337–369, 2010.

[11] J. Eckstein and D. P. Bertsekas, "On the Douglas–Rachford splitting method and the proximal point algorithm for maximal monotone operators," Math. Program., vol. 55, no. 1, pp. 293–318, Jun. 1992.