IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 3, Issue 4 (July-Aug. 2012), PP 01-06
www.iosrjournals.org

Fraud and Tamper Detection in Authenticity Verification through Gradient Based Image Reconstruction Technique for Security Systems

[1]Sonal Sharma, [2]Preeti Tuli
[1, 2]*(Computer Science & Engineering, DIMAT,India)*

Abstract **:** *Authenticity verification for security systems is a very important research problem with respect to information security. One of the principal problems in image forensics is determining if a particular image is authentic or not. This can be a crucial task when images are used as basic evidence to influence judgment like, for example, in a court of law. Image editing software like Adobe Photoshop, Maya etc. and technically advanced digital photography are used to edit, manipulate or tamper the images easily without living obvious visual clues. The abusive use of digital forgeries has become a serious problem in various fields like authenticity verification, medical imaging, digital forensic, journalism, scientific publications etc. To carry out such forensic analysis, various technological instruments have been developed in the literature. In this paper the problem of detecting if an image has been forged is investigated. To detect tampering and forging, a novel methodology based on gradient based image reconstruction is proposed. Our method verifies the authenticity of image in two phases- modeling phase; where the image is reconstructed from its gradients by solving a poisson equation and forming a knowledge based model and simulation phase; where the absolute difference method and histogram matching criterion between the original and test image is used. Such a method allows concluding that if a tampering has occurred. Experimental results are presented to demonstrate the performance of our gradient-based image reconstruction approach and confirm that the technique is able to verify whether a forged image is presented to a security system for authenticity verification. Through this unique mechanism, one can secure the most reliable information and forging or tampering of images for gaining false authentication and hence fraud can be detected.*

Keywords: *Gradient, Poisson equation, Region of interest (ROI), Digital image forensics, Authenticity verification.*

I. INTRODUCTION

In recent times most of the researchers are working on mechanisms adopted for information security, because it is always of great concern for human kind. Digital crime and increasing fraud in security systems along with constantly emerging software technologies, is growing at a very faster rate. By observing a digital content as a digital clue, multimedia forensics aims to introduce novel methodologies to support clue analysis and to provide an aid for making a decision about a crime. Multimedia forensics [1], [2], [3] deals with developing technological instruments operating in the absence of watermarks [4], [5] or signatures inserted in the image. In fact, different from digital watermarking, forensics means are defined as “passive” because they can formulate an assessment on a digital document by resorting only to the digital asset itself. These techniques basically allow the user to determine if particular content has been tampered with [6], [7] or which was the acquisition device used [8], [9]. In particular, by focusing on the task of acquisition device identification, two main aspects must be studied: the first is to understand which kind of device has generated a digital image (e.g. a scanner, a digital camera or is a computer graphics product) [10], [11], while the second is to determine which specific camera or scanner (by recognizing model and brand) acquired that specific content [8], [9].

The other main multimedia forensics topic is image tampering detection [6] that is assessing the authenticity of a digital image. Information integrity is fundamental in a trial, but it is clear that the advent of digital pictures and relative ease of digital image processing today makes this authenticity uncertain. Modifying a digital image to change the meaning of what is represented in it can be crucial when used in a court of law where images are presented as basic evidence to influence the judgment. Furthermore, it is interesting, once established that something has been manipulated, to understand exactly what happened: if an object or a person has been covered, if a part of the image has been cloned, if something has been copied from another image, or if a combination of these processes has been carried out. In this paper, this issue is investigated, and the proposed method is able to detect that whether tampering has taken place.

The rest of the paper is organized as follows: Section 2 reviews the problem formulation and solution methodology. Section 3 presents the experimental results and outcomes. Section 4 deals with the conclusion and future work.

II. PROBLEM FORMULATION AND SOLUTION METHODOLOGY

The problem of fraud detection has been faced by proposing different approaches each of these based on the same concept: a forgery introduces a correlation between the original image and the tampered one. Several methods search for this dependence by analyzing the image and then applying a feature extraction process. Reconstruction of the original test image has not been so far used for tamper detection.

In [12] grayscale reconstruction has been formally defined for discrete images. Its authors have underscored relations to binary reconstruction and morphological geodesic transformations. In [13] another approach for image reconstruction from local phase vectors in the monogenic scale space is presented. In [14] fan-beam image reconstruction algorithm is presented by the authors who reconstruct an image via filtering a back projection image of differentiated projection data. In [15] a new method for the exact image reconstruction from projections is proposed. The original image is projected into several view angles and the projection samples are stored in an accumulator array. In [16] another novel approach is presented which consists first in using an off-the-shelf image database to find patches visually similar to each region of interest of the unknown input image, according to associated local descriptors which are then warped into input image domain according to interest region geometry and seamlessly stitched together. Final completion of still missing texture-free regions is obtained by smooth interpolation.

None of these approaches [12, 13, 14, 15, and 16] conducts gradient maps in the image reconstruction. The approach presented in this paper verifies the authentication in two phases: in phase one (modeling phase), the image is reconstructed from the image gradients by solving a Poisson equation and in the phase two (simulation phase) absolute difference method and histogram matching criterion between the original and test image is used.

1.1 Poisson Image Reconstruction Using Image Gradients

Image reconstruction from gradient fields is a very active research area. The gradient-based image processing techniques and the poisson equation solving techniques have been addressed in several related areas such as high dynamic range compression [17], Poisson image editing [18], image fusion for context enhancement [19], interactive photomontage [20], Poisson image matting [21] and photography artifacts removal [22].

In our approach, a new criterion is developed, where the image is reconstructed from its gradients by solving a poisson equation and hence used for authenticity verification.

In 2D, a modified gradient vector field:

$$G' = [G'x, G'y] \tag{1}$$

may not be integrable.

Let I' denote the image reconstructed from G', we employ one of the direct methods recently proposed in [17] to minimize:

$$\|\nabla I' - G\| \tag{2}$$

so that:

$$G \approx \nabla I' \tag{3}$$

By introducing a Laplacian and a divergence operator, I' can be obtained by solving the Poisson differential equation: [24, 25]

$$\nabla^2 I' = \mathrm{div}([G'_x, G'_y]) \tag{4}$$

Since both the Laplacian and div are linear operators, approximating those using standard finite differences yields a large system of linear equations. We use the full multigrid method [23] to solve the Laplacian equation with Gaussian-Seidel smoothing iterations [25]. For solving the Poisson equation more efficiently, an alternative is to use a rapid Poisson solver [25], which uses a sine transform based on the method [24] to invert the Laplacian operator. However, the complexity with the rapid Poisson solver will be O(n(log(n))). Therefore, the full multigrid method [23] is employed in our implementation. The image is zero-padded on all sides to reconstruct the image

.

1.2 Absolute Difference

In the present work our approach is to find the absolute difference between the original and the reconstructed image. Subtraction gives the difference between the two images, but the result may have a negative sign and can be lost. The function that finds how different the two images are- regardless of the arithmetic sign- is the absolute difference:

$$N(x, y) = |O_1(x, y) - O_2(x, y)| \tag{5}$$

where, O_1 (x, y) and O_2(x, y) are pixels in the original images, |x| is the absolute difference operator, and N(x, y) is the resultant new pixel. The absolute difference operator returns +x whether the argument is –x or +x.

1.3 Histogram Normalization

Histogram is a graphical representation of the intensity distribution of an image. It quantifies the number of pixels for each intensity value considered. Histogram Equalization is a method that improves the contrast in an image, in order to stretch out the intensity range. Equalization implies mapping one distribution (the given histogram) to another distribution (a wider and more uniform distribution of intensity values) so that the intensity values are spread over the whole range.

To accomplish the equalization effect, the remapping should be the cumulative distribution function (CDF)

For the histogram H(i), its cumulative distribution H'(i) is:

$$H'(i) = \Sigma\, H(j), \text{ where } 0 \leq j < i \qquad (6)$$

To use this as a remapping function, we have to normalize H'(i) such that the maximum value is 255 or the maximum value for the intensity of the image). Finally, we use a simple remapping procedure to obtain the intensity values of the equalized image:

$$\text{equalized}(x, y) = H'(\text{src}(x,y)) \qquad (7)$$

In our work first we perform the histogram normalization and then the histogram equalization criteria is used where the normalized histogram values of the original and test image are utilized for matching the two images. The proposed research work has two different phases: modeling phase and simulation phase. The schematic workflow diagram for the modeling phase has been shown in the Fig. 1.

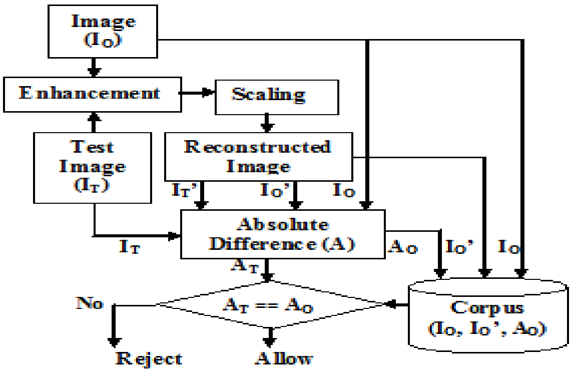


Figure 1: Schematic diagram for Modeling and Simulation Phase

In the modeling phase, first an input image (I_O) is enhanced and scaled for the removal of distortion with loss-less information, and then the poisson image reconstruction from image gradients technique is applied to obtain the reconstructed image(I_O'). Now the absolute difference (A_O) of the image and reconstructed image is obtained and the results are stored in corpus for matching the test data. In the simulation phase, the model has been utilized for simulating trained and test patterns. To summarize this simulation process first a test image (I_T) is studied with proper enhancement. In the enhancement stage removal of noise from the image has been carried out and then it is reconstructed using the proposed reconstruction technique to obtain reconstructed image (I_T') and then the absolute difference between I_T and I_T' is calculated to obtain A_T. (For a particular subject A_O is stored in the corpus which is retrieved during simulation phase for the comparison). Finally, A_T is compared with A_O and the results are obtained which may allow or reject the subject and hence his authenticity verification is completed.

2.4 Algorithm used

The methodology adopted in the present paper has been depicted below:

Algorithm 1: Modeling and Simulation of original and reconstructed image

Modeling phase

Step 1: Read an image (I_O).
Step 2: Convert into grayscale image, say R.
(Enhancement stage)
Step 3: Perform Scaling on the image.
Step 4: Enhance the image using median filtering and convolution theorem (I_O).
Step 5: Reconstruct the image using proposed methodology (I_O').
Step 6: Find the absolute difference between original and reconstructed image (A_O).
Step 7: Store the original image, reconstructed image and absolute difference (I_O, I_O', A_O)

Simulation phase

Step 8: Input a test image (I_T)
Step 9: Reconstruct I_T to obtain I_T' and find the absolute difference (A_T) between I_T and I_T'
Step 10: Compare A_T and A_O to find a match and hence allow or reject the subject accordingly.

A. Modeling and Simulating

In the *modeling phase*, let I_O be the original image of a subject which has to be modeled for the formation of knowledge based corpus. After enhancing and proper scaling of the original image I_O, the image is poisson reconstructed from its gradients as:

I_O’ = Poisson_reconstruction (I_O) (8)

Now the absolute difference between the original and reconstructed image is calculated as :

A_O = Absolute_difference (I_O, I_O’) (9)

Now store the triplet (I_O, I_O’, A_O) in the corpus so as to form the knowledge based model (corpus). The equations (8) and (9) can be repeatedly used to register n number of subjects, and store their details for authentication verification.

In the *simulation phase*, when the tampered or forged image will be presented to the security system for authentication, the system will reconstruct the test image (I_T) as:

I_T’ = Poisson_reconstruction (I_T) (10)

And then the absolute difference between the original test image (I_T) and reconstructed test image (I_T’) is calculated as:

A_T = Absolute_difference (I_T, I_T’) (11)

Now the resultant A_T is compared with A_O (the absolute difference stored in corpus of the original and reconstructed original image in modeling phase)

```
If ($A_T$ == $A_O$)
    “Authenticity Verified as TRUE!”
Else
    “Authenticity Verified as FALSE!”
```

Hence, the result will reject the subject due to a mismatch and the images obtained by forgery or tampering for authenticity verification will be regarded as fake or invalid and any hidden data (for destroying the security system or secret communication) will be clearly identified.

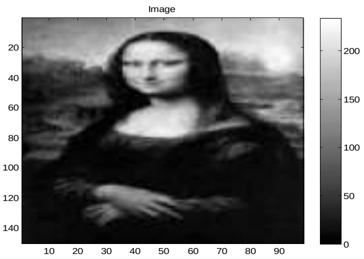
III. EXPERIMENTAL RESULTS AND OUTCOMES

The solution methodology for the above stated problem is implemented using soft computing tools and the experimental outcomes are shown in Fig. 2.

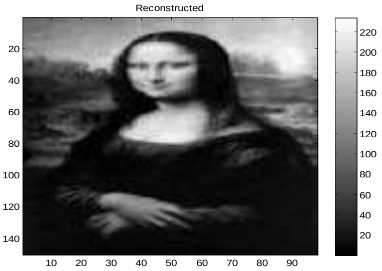
As show in Fig. 2, the original image is passed through the modeling phase steps mentioned in Algorithm 1 and the results are shown in Fig. 2 (2.1) to (2.6). Now the corpus contains the triplet (I_O, I_O’, A_O) for the registered subject’s original image.

(2.1)

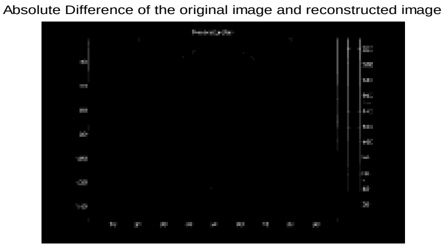
(2.2)



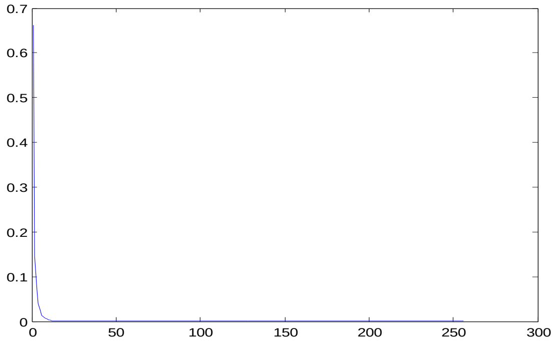
(2.3)



(2.4)

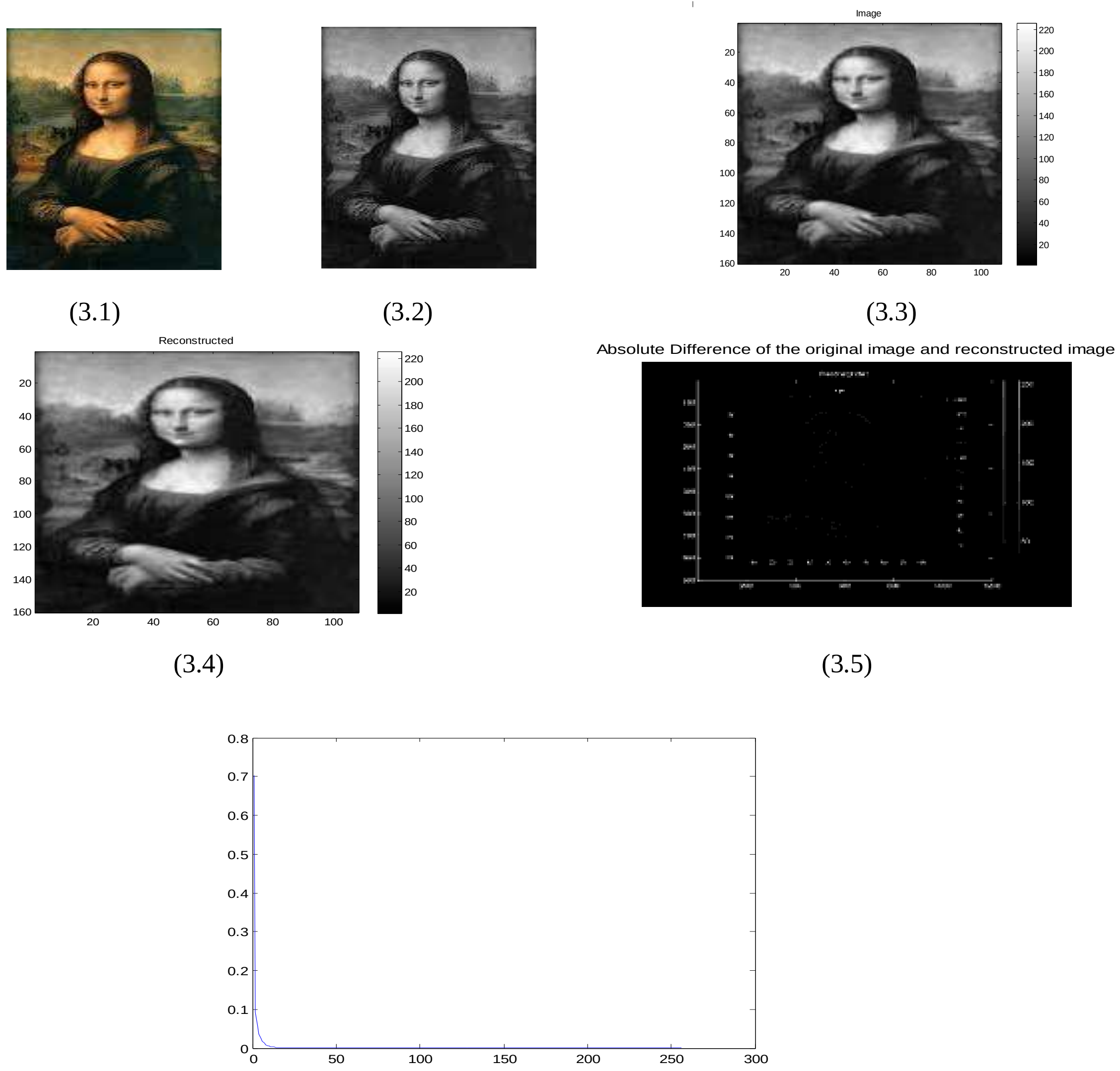


(2.5)



(2.6)

Figure 2: Results for modeling phase (Original Image): (2.1) Original Image (I_O), (2.2) Grayscale Image, (2.3) Enhanced and Scaled Image, (2.4) Reconstructed Image (I_O'), (2.5) Absolute difference (A_O) of I_O and I_O', (2.6) Normalized Histogram of absolute difference shown in (2.5).



(3.1) (3.2) (3.3)

(3.4) (3.5)

(3.6)

Fig. 3: Results for simulation phase [Test (tampered) Image]: (3.1) Original Image (I_T), (3.2) Grayscale Image, (3.3) Enhanced and Scaled Image, (3.4) Reconstructed Image (I_T'), (3.5) Absolute difference of I_T and I_T', (3.6) Normalized Histogram of absolute difference shown in (3.5).

As shown in Fig. 3, the test image (tampered) is passed through the steps of simulation phase mentioned in Algorithm 1and the results are shown in Fig. 3 (3.1) to (3.6). Next the histogram of absolute difference obtained in Fig. 3 (3.6) is normalized and compared with the normalized histogram of original image shown in Fig. 2 (2.6), and the so obtained result is *inequality,* since, the value of the difference is not zero and comes to be 0.0049, and hence the image is declared as tampered and finally rejected. If the image was not tampered then, the so obtained difference (between the normalized histogram of absolute difference of the test image and reconstructed test image (Fig. 3.6) and the normalized histogram of absolute difference of the original image and reconstructed original image (Fig. 2.6) would be 0.00

In this manner the authenticity of the individual's can be verified and the test images can be classified as tampered (or forged) or original, and hence the tampering can be detected.

IV. CONCLUSION AND FURTHER WORK

A novel gradient-based image reconstruction algorithm by solving poisson equation for detecting image tampering in authenticity verification has been proposed in this paper. Our authenticity verification approach is conducted in two phases. At first, the image is reconstructed from the gradients by solving a poisson equation, and next normalized histogram criterion and absolute difference method is used to match the original and test image. Experimental results demonstrate both the feasibility and the efficiency of our algorithm.

REFERENCES

[1] S. Lyu and H. Farid, "How realistic is photorealistic?," IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 845–850, 2005.

[2] H. Farid, "Photo fakery and forensics," Advances in Computers, vol. 77, pp. 1–55, 2009.

[3] J. A. Redi, W. Taktak, and J. L. Dugelay, "Digital image forensics: a booklet for beginners," Multimedia Tools and Applications, vol. 51, no. 1, pp. 133–162, 2011.

[4] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital watermarking. San Francisco, CA: Morgan Kaufmann, 2002.

[5] M. Barni and F. Bartolini, Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. Marcel Dekker, 2004.

[6] H. Farid, "A survey of image forgery detection," IEEE Signal Processing Magazine, vol. 2, no. 26, pp. 16–25, 2009.

[7] A. Popescu and H. Farid, "Statistical tools for digital forensics," in Proc of Int.'l Workshop on Information Hiding, Toronto, Canada, 2005.

[8] A. Swaminathan, M. Wu, and K. Liu, "Digital image forensics via intrinsic fingerprints," IEEE Transactions on Information Forensics and Security, vol. 3, no. 1, pp. 101–117, 2008.

[9] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise," IEEE Transactions on Information Forensics and Security, vol. 3, no. 1, pp. 74–90, 2008.

[10] N. Khanna, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Forensic techniques for classifying scanner, computer generated and digital camera images," in Proc. of IEEE ICASSP, Las Vegas, USA, 2008.

[11] R. Caldelli, I. Amerini, and F. Picchioni, "A DFT-based analysis to discern between camera and scanned images," International Journal of Digital Crime and Forensics, vol. 2, no. 1, pp. 21–29, 2010.

[12] Luc Vincent, "Morphological Grayscale Reconstruction in Image Analysis: Applications and Efficient Algorithms" IEEE Transactions on Image Processing, vol. 2, no. 2, 1993.

[13] Di Zang and G. Sommer, "Phase Based Image Reconstruction in the Monogenic Scale Space" DAGM-Symposium, 2004.

[14] S. Leng, T. Zhuang, B. Nett and Guang-Hong Chen, "Exact fan-beam image reconstruction algorithm for truncated projection data acquired from an asymmetric half-size detector" Phys. Med. Biol. 50 (2005) 1805–1820.

[15] A. L. Kesidis, N. Papamarkos, "Exact image reconstruction from a limited number of projections" J. Vis. Commun. Image R. 19 (2008) 285–298.

[16] P. Weinzaepfel, H. Jegou, P. Perez, "Reconstructing an image from its local descriptors " Computer Vision and Pattern Recognition (2011).

[17] R. Fatta, D. Lischinski, M. Werman, "Gradient domain high dynamic range compression" ACM Transactions on Graphics 2002;21(3):249-256.

[18] P. P´erez ,M. Gangnet , A. Blake, " Poisson image editing" ACM Transactions on Graphics 2003;22(3):313-318.

[19] R. Raskar, A. Ilie , J.Yu, " Image fusion for context enhancement and video surrealism", In: Proceedings of Non-Photorealistic Animation and Rendering '04, France, 2004. p. 85-95.

[20] A. Agarwala , M. Dontcheva, M. Agrawala , S. Drucker, A.Colburn, B. Curless, D Salesin , M. Cohen M, " Interactive digital photomontage. ACM Transactions on Graphics" 2004;23(3):294-302.

[21] J. Sun, J. Jia, CK. Tang , HY Shum , "Poisson matting. ACM Transactions on Graphics" 2004;23(3):315-321.

[22] A. Agrawal , R. Raskar, SK. Nayar , Y. Li, "Removing flash artifacts using gradient analysis" ACM Transactions on Graphics 2005;24(3):828-835.

[23] W. Press, S. Teukolsky, W. Vetterling, B. Flannery "Numerical Recipes in C: The Art of Scientific Computing" Cambridge University Press; 1992.

[24] R. Raskar, K. Tan, R. Feris , J. Yu, M. Turk "Non-photorealistic camera: depth edge detection and stylized rendering using multi-flash imaging" ACM Transactions on Graphics 2004;23(3):679-688.

[25] J. Shen, X. Jin, C. Zhou, Charlie C. L. Wang, "Gradient based image completion by solving the Poisson equation," PCM'05 Proceedings of the 6th Pacific-Rim conference on Advances in Multimedia Information Processing – Volume Part I 257-268