Study and Analysis of Image Reconstruction Techniques for Fraud and Tamper Detection in Authenticity Verification

Sonal Sharma, Preeti Tuli

Abstract: Image reconstruction is a very important research problem with respect to information security. Digital image reconstruction is a robust means by which the underlying images can be revealed and analyzed for any fraud. One of the principal problems in image forensics and security systems 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. 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 such tampering, a novel methodology based on image reconstruction is proposed. Such a method allows understanding with high reliability whether an attack has occurred.

Index Terms: Gradient, Poisson equation, Region of interest (ROI), Digital image forensics, Authenticity verification, Image reconstruction from projections

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 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 II reviews the various image reconstruction techniques and formulates the problem. Section III presents the solution methodology. Section IV presents the proposed outcome. Section V deals with the conclusion and further planning of the work.

II. PROBLEM FORMULATION

One of the most common applications of image manipulations is presenting a tampered image for authenticity verification to a security system, for instance taking photograph of a subject without his knowledge and presenting for fake authentication or sending hidden destructive data to a security system by hiding it in an image for system destruction. The system matches the features of the input test image with those of the one stored in corpus and allows the attacker as authentic user. When this tampering is done with care it is very difficult to detect. Moreover, since the image is of the same subject, some components will be similar with the original image and thus will not be detectable using methods that look for incompatibilities in statistical measures in different parts of the image. 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.

Revised Manuscript Received on 30 August 2012.
* Correspondence Author

Sonal Sharma, Computer Science & Engineering, , Disha Institute of Management & Technology, Raipur, India.

Preeti Tuli, Computer Science & Engineering, Disha Institute of Management & Technology, Raipur, India.

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.

As per the literature, the methods that have been applied so far are not based on soft-computing tools. Very little amount of work has been carried out with knowledge-based or model-based using soft-computing tools like artificial neural network (ANN) and fuzzy logic. The approach that has been applied for the problem is completely model-based or knowledge-based. In the present research work, the simulation has to be done in near future to justify the image reconstruction system for security and tamper detection through proposed image reconstruction technique.

In the present paper the problem has been formulated in eight stages i.e. there are eight problems that can be associated with security system for fraud and temper detection through image reconstruction mechanism with proper employment of soft-computing technique. The first problem is the removal of noises and loss-less information in the image. Due to presence of noise the performance of the system may degrade. Thus it must be removed and hence compressed, for obtaining better results during simulation process for security. The second problem is the employment of proper scaling of the image. The fourth problem is to reconstruct the image after employing proposed reconstruction mechanism. The fifth problem is finding the absolute difference of the original and reconstructed image. The seventh problem is framing of knowledge-based model as corpus for security system. The eighth problem is the simulation for security for proper authentication and authorization of trained and test patterns and also its final observations. The proposed work aims to analyze and discuss experimentally the aforesaid problem in the subsequent subsections.

III. PROPOSED SOLUTION METHODOLOGY

The detection of tampering in a given image, known as tampering detection, is an important task in forensics and security systems. A novel gradient-based image reconstruction algorithm by solving Poisson equation has been proposed in this paper. Our image completion approach is conducted in two phases. At first, the gradient maps of the image are reconstructed by incorporating gradient factors. After determining the gradient maps, the reconstruction result is computed from the gradients by solving a Poisson equation. Experimental results in future work will demonstrate both the feasibility and the efficiency of our algorithm. Thus, the mechanism of poisson image reconstruction from image gradients has been adopted for fraud detection and security system.

A. Poisson Image Reconstruction Using Image Gradients

The gradient-based image processing techniques and the poisson equation solving techniques have been addressed in several related areas. In our approach, a new criterion is developed, where the image can be reconstructed from its gradients by solving a Poisson equation and hence used for authenticity verification.

Image reconstruction from gradient fields is a very active research area.

In 2D, a modified gradient vector field,

$$G' = [G'_x, G'_y] \quad (1)$$

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,

$$\| \nabla I' - G \| \quad (2)$$

so that,

$$G \approx \nabla I' \quad (3)$$

By introducing a Laplacian and a divergence operator, I' can be obtained by solving the Poisson differential equation [19, 20]

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

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 [18] to solve the Laplacian equation with Gaussian-Seidel smoothing iterations [21]. For solving the Poisson equation more efficiently, an alternative is to use a rapid Poisson solver [21], which uses a sine transform based on the method [19] to invert the Laplacian operator. However, the complexity with the rapid Poisson solver will be O(n(log(n))). Therefore, the full multigrid method [18] is employed in our implementation. The image is zero-padded on all sides to reconstruct the image I'

As little amount of work has been done in this area, using soft-computing techniques, hence through the present research work, commendable and remarkable results have to be obtained through the mechanism of image reconstruction using soft-computing techniques. 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

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 an unknown image (I_T) is studied with proper

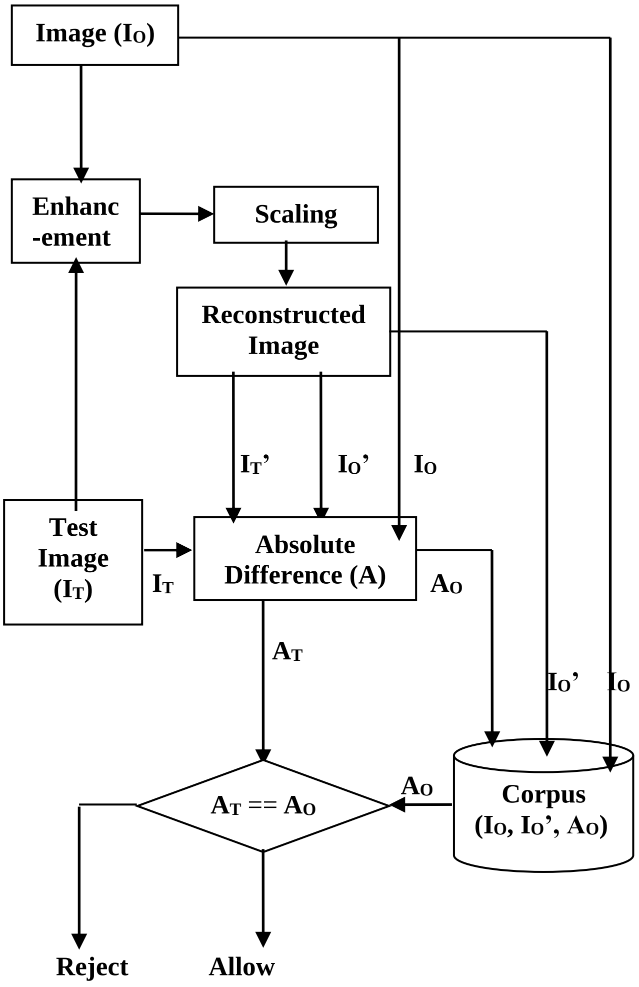

Fig. 1: Schematic diagram for Modeling and Simulation Phase enhancement.

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 (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.

B. The 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.
Step4: 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.

IV. THE PROPOSED OUTCOME

When the tampered or forged image will be presented to the security system for authentication the system will reconstruct the test image and calculate the absolute difference between the original test image and reconstructed test image. The result will be then compared with the absolute difference stored in corpus (of the original and reconstructed original image in modeling phase). The result will reject the subject due to mismatch. Hence 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.

V. CONCLUSION AND FURTHER WORK

As stated earlier the above proposed methodology upon implementation may result into proposed outcome stated in above section.

In the present paper soft-computing techniques has to be applied for proper simulation and analysis. The simulation part has to be carried out using considerable and acceptable tools of soft-computing techniques to justify the security system.

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. W. Press, S. Teukolsky, W. Vetterling, B. Flannery "Numerical Recipes in C: The Art of Scientific Computing" Cambridge University Press; 1992.
19. 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.
20. A. Agrawal, R. Raskar, S. K Nayar , Y. Li, " Removing flash artifacts using gradient analysis" ACM Transactions on Graphics 2005;24(3):828-835.
21. 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

AUTHOR PROFILE

Sonal Sharma did Bachelors of Engineering in 2009 in Computer Science & Engineering (Honors) from DIMAT, Raipur, and pursuing Masters of Technology in Information Security from DIMAT, Raipur.

Preeti Tuli did Bachelors of Engineering in 2000 in Computers from Shri Govind Ram Sakseria Institute of Technology and Scince, Indore, and M.Tech(CSE) from RCET, Bhilai**i**

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)