A Novelty Approach on Forgery Digital Image Detection based Image Source Identification ANN

K. Muthu Kumar

Assistant Professor, Department of Computer Science and Engineering,
PSN Engineering College, Tirunelveli (T.N.), India,

Abstract

In imaging science, the photo editing software packages can alter the original images without any detecting traces of tampering. Hence, the image forgery detection technique plays an important role in verifying the integrity of digital image forensics for authentication. The techniques such as watermarking are used for authentication but it can be modified through third parties attack through extraction. Malicious and digital imaging (digital products) tamper detection is the subject of this article. In particular, we focus on a special type of digital forgery detection - copy attack campaign, in which part of the image is copied and pasted into the image and the cover features a large image of intentions another. In this paper, we investigate the dynamic forged copy detection problem, and describes a highly efficient and reliable detection method that based on image source ANN identification.. Even when the region is enhanced copy / retouching and background merger, and the method can successfully identify counterfeit forgery when images are saved in a lossy format (such as JPEG). The performance of the method's performance several forged images.

Keywords*:Forgery detection, image source identification, forgery, tamper detection, spoof attacks.*

I.Introduction

JPEG image format is widely used in most digital cameras and image processing software. In general, JPEG compression introduce block effects. Digital cameras and image processing software manufacturers often use different JPEG quantization table to balance the compression ratio and image quality. This difference also resulted in images obtained by different block effect. When creating a fake number, so that the image can be manipulated to inherit a variety of different sources compression equipment. These inconsistencies, if detected, can be used to check the integrity of the image. In addition, the process to create fake artifacts also changed the locks because the processing operations blockiness block changed greatly affected, such as image stitching, sampling and local operations, such as the goal to optimize skin. Thus, the discrepancy can block artifacts in the image story of a given image has undergone found. For fake photos practices may be as old as photography itself art. Digital photography and image editing software, powerful makes it very easy nowadays to create believable digital image was forged, even non-professional. As digital photography continues to replace its analog correspondence, rapidly increasing need for reliable detection of digital image tampering. Check the digital image content or to identify counterfeit area, digital photos are used as evidence, apparently, for example in the law, the court is useful. In this paper, we propose a passive way through JPEG blockiness measure on the basis of inconsistent quality, digital image forgery detection. Is first estimated based on the histogram of the DCT coefficients introduced in the power spectrum of the new

DOI:10.5121/ijcsa.2015.5105

quantization table, and the locking means are provided in the table based on the calculation. Inconsistent blockiness review images in JPEG format traces forged. The proposed method can be detected using different quantization tables in the mosaic image forgery or counterfeit product may cause blocking artifacts in the image of the range block as inconsistency and modifications that do not match the object.

Fig 1. Example for Digital Image Forgery

In addition, our proposed quantization table than maximum likelihood estimation algorithm based approach is much faster. Obviously, the detection of complex numbers are forged, the question is no universal solution. What is needed is a group that can be applied to all images in the hands of different tools. Then on the authenticity determination is achieved by using the results obtained in different ways by the explanation. This cumulative evidence is inadequate to provide a convincing argument, everyone's methods cannot. In this work, a new method for the detection of the picture processing based on each of the pattern noise, digital camera sensor is inadvertently inserted into the need to make each image. The method is applicable whenever we claimed to forge an image when we have already taken, or at least, we must take the camera does not have a camera image circumstances. Since pattern noise appears to be a random number unique fingerprint of the image sensor [7], [8], can determine the consistency of the residual noise detected by the sensor element of the pattern noise particularly in the forged part yes. From the early general image, which has been accepted as evidence of the occurrence of the event represented. And other computer areas become more common, accepted digital image files has become a common practice. Low-cost hardware and software tools available, you can easily create, modify and manipulate digital images has been no obvious signs of these operations. Therefore, we are rapidly reaching the case, you cannot shoot the integrity and authenticity of digital images are taken for granted. This trend undermines the digital images as evidence in court, such as the credibility of the news reports, as part of the medical records or financial documents, as it may not be possible to distinguish between a given digital images whether original or modified version of or in real life events and objects even said. Digital image is an issue fake criminal cases and public courses increasingly serious. Currently, there is no established method to verify the authenticity and integrity of the automatic mode digital images. Digital image forgery detection is an important impact on the number [1] image of credibility new research fields. In the past period of time a large number of digital image processing, you can see on the tabloid magazines, the fashion industry, scientific journals, court room, major media and deception photos receive our mail. For the detection of forged digital image technology is divided into active and passive [3]. Active focus, digital images, require some pre-processing, for example, when a watermark embedded in an image, or create a signature generation, which would limit their application in real time. In addition, there are tens of millions of digital images on the Internet without a digital signature or watermark. In this case, the activity of the image cannot be used to find the authentication. Unlike the method based on the signature,

and, in accordance with the watermark; passive technologies advance [4] does not generate a digital signature or the embedded watermark. There are three widely-used techniques for processing digital images [3]. 1) Action - is an image of the operation to achieve specific results. 2) Fused (Composition) - a common form of a photographing operation in the digital images of two or more connections to a single compound 3) clone (copy, move).

II.Related Work

In this literature review, Recent advances in digital forensics, leading to a number of techniques to detect the photo processing. These methods include for detecting clones [1], [2]; splicing [3]; resampling artifacts [4], [5]; aberration of color filter array [6]; camera sensor noise interference pattern [7]; colors [8] aberration; illumination inconsistencies [9] - [11]. Although very effective in some cases, many of these techniques only apply to a relatively high-quality images. Forensic analysis, however, are often faced with poor quality images at a resolution and / or compression. Therefore, it is necessary to take forensics tools, is specifically applicable to the advantages of the detection process low-quality image. This is particularly difficult because of the low quality images are often damaged, can be used to detect tampering with statistical artifacts. A complementary approach to detect tampering low quality images presented here. This method is to be inserted into a portion of the higher quality JPEG image in JPEG image is detected, for example, results of the operation, when a person's head is joined to another body of the person, or if the two are combined in one shot single compound. The working principle of this method is an explicit part of the image is determined by the original image is compressed in the rest phase, the lower the quality.Compared to [12], our method does not require estimates of the discrete cosine transform (DCT), quantization, a portion from a so-called original image. Only quantitative estimate of the underlying DCT coefficients in the calculation is trivial and error-prone to some estimates, resulting in Forensic analysis of vulnerabilities. Compared to [13], our method does not require the image segmentation in order to detect inconsistencies blocked. Moreover, our method can detect local operation and global approach [13], which is generally only detect crop and compression. And compared to [14], our approach, although it may not so powerful, much more computationally simpler and does not require a large database of images to form a support vector machine (SVM). As with all forensic analysis, each technology has its advantages and disadvantages. The new technology presented here will help increase the number of forensic tools based on JPEG artifacts, but should be a new tool in the arsenal of forensic analysis is useful. Consider creating a fake movie presents two stars, is rumoured to be involved in a romantic walk on the beach at sunset. Personal image this image can be spliced together to establish for each actor. In doing so, it is often difficult to exactly match the lighting effects, due to the directional light (for example, in a clear day, the sun). Differences in lighting, which can be a warning signal of digital manipulation. As shown in Figure 1, for example, significant light in which the composite image in two different positions, respectively, the first shooting. Although this type of forgery is quite obvious and more subtle differences in lighting direction may be difficult to use simple visual inspection to detect. As the direction of the light source can be estimated for different object / image of a person, the inconsistency in the direction of illumination can be used as evidence for digital processing. This article describes a technique from a single image estimate the direction of the light source, and shows its true environmental benefits at. Fraud often involves creating a digital image synthesis from a single object / person. By doing so, difficult accurate lighting effects to match, due to the lighting direction (for example, in a clear day, the sun). At least one reason for this is that this manipulation may be required to create shadows and lighting gradient or destroyed. Although large irradiation direction can be quite obvious inconsistency, there is physical evidence of human psychology literature is surprisingly human subjects insensitive lighting differences entire image. As the direction of the light source can be estimated for different object / image of a person, the illumination can be used as digital evidence

tampering inconsistent. We have described a technique for the illumination light source is estimated from the direction (in one degree of freedom) of the. This technique is based on the work of [6] described. We relaxed some simplifying assumptions, it is necessary to make the problem tractable, and the inductive method under local sources (such as light bulbs) work to extend this basic recipe. Synthetically produced and displayed at the real image, the effectiveness of this technique. We are currently investigating how the light source can be used to estimate the direction of the geometrical image of the third component in N_z (plane, sphere, cylinder, etc.) in the known surface. If successful, this approach would eliminate the current ambiguity in the estimated source. We are also a technology that automatically determine which mode, unlimited or local best describes the basic forensic analysis of image content must decide which mode to use, because the current situation.

III.IMAGE SOURCE IDENTIFICATION

Generation of image recognition image source survey design techniques to identify characteristics of digital data acquisition devices (eg, digital cameras, camcorders and scanners) used in. It is expected that these techniques to achieve the two main effects. The first class (model) the source characteristics, and the second is the property of a single source. Basically, the results of both refer to two different operating configurations. In determining the properties of the class, in general, a single image can be used to evaluate and source information is extracted by image analysis. Properties obtained in a single source, however, is known, or an image obtained from a number of potential sources of both the image and the source apparatus that can be used to evaluate and analyze the image to determine whether the characteristics of the source concerned. Successful identification techniques depending on the assumption that all the source images acquired by the image acquiring unit of the apparatus showing an image acquisition device of some inherent characteristics, due to their (own) piping whether the training images and the image content of the display unique hardware components. (Note that this device normally encodes the relevant device information, such as the model, type, date and time, and image compression of the header of the details, for example, in the EXIF header, however, because this information can be easily be modified or deleted, cannot be used for forensic purposes.) Due to the popular image of a digital camera, the researchers focused on research to identify the source of a digital camera and scanner identification is only the beginning.

IV.METHODOLOGY

Digital Image are fake so real, they do not leave any evidence of tampering, and may be associated with the real picture, there is no difference. Forgery digital image processing so that the digital image data are highly correlated. In this article, we take advantage of this feature by using a similar feature vector regression (AR) coefficients car, a digital image of the sample in order to determine the location of forgery. 300 different image feature vectors are used to train artificial neural network (ANN) and artificial neural networks and other features vector test 300.

The follow formula represents the neural network:

$$f(x) = \sigma(W_o \square \sigma(W_H \times X^T)) \qquad (1)$$

Now we can calculate the partial differential of the network with respect to the weight on hidden unit i that receives input j. This will us to calculate the update for the weight.

$$\frac{\partial f(x)}{\partial w_{ij}} = \frac{\partial \sigma(W_o \square \sigma(W_H \times X^T))}{\partial w_{ij}} \quad (2)$$

$$= \sigma(W_o \square \sigma(W_H \times X^T))(1-\sigma(W_o \square \sigma(W_H \times X^T)) \frac{\partial W_o \square \sigma(W_H \times X^T)}{\partial w_{ij}}$$

$$= (Y_o)(1-Y_o) \frac{\partial W_o \square \sigma(W_H \times X^T)}{\partial w_{ij}} \quad (3)$$

$$= (Y_o)(1-Y_o) \frac{\partial w_{o,i} \sigma(W_{H,i} \times X^T)}{\partial w_{ij}} \quad (4)$$

$$= (Y_o)(1-Y_o) w_{o,i} \sigma(W_{H,i} \times X^T)(1-\sigma(W_{H,i} \times X^T)) \frac{\partial (W_{H,i} \times X^T)}{\partial w_{ij}} \quad (5)$$

$$= (Y_o)(1-Y_o) w_{o,i} Y_i (1-Y_i) \frac{\partial (W_{H,i} \times X^T)}{\partial w_{ij}} \quad (6)$$

$$= (Y_o)(1-Y_o) w_{o,i} Y_i (1-Y_i) x_j \quad (7)$$

To update weights on the output unit the calculate is simpler:

$$\frac{\partial f(x)}{\partial w_{oi}} = \frac{\partial \sigma(W_o \square \sigma(W_H \times X^T))}{\partial w_{oi}} \quad (8)$$

$$= \sigma(W_o \square \sigma(W_H \times X^T))(1-\sigma(W_o \square \sigma(W_H \times X^T)) \frac{\partial W_o \square \sigma(W_H \times X^T)}{\partial w_{oi}} \quad (9)$$

$$= (Y_o)(1-Y_o) \frac{\partial W_o \square \sigma(W_H \times X^T)}{\partial w_{oi}} \quad (10)$$

$$= (Y_o)(1-Y_o) Y_i \quad (11)$$

$$f(x_1,...,x_n) = \frac{\sum_{k=1}^{m} b^k [\prod_{i=1}^{n} \mu_{A_i^k}(x_i)]}{\sum_{k=1}^{m} [\prod_{i=1}^{n} \mu_{A_i^k}(x_i)]} \quad (12)$$

$$E^p = \frac{1}{2}[f(x_1^p,...,x_n^p) - y^p]^2 \quad (13)$$

$$b^k(t+1) = b^k(t) - \theta \frac{\partial E^P}{\partial b^k}\bigg|_t \quad (14)$$

$$\sigma^k(t+1) = \sigma^k(t) - \theta \frac{\partial E^P}{\partial \sigma^k}\bigg|_t \quad (15)$$

$$a^k(t+1) = a^k(t) - \theta \frac{\partial E^P}{\partial a^k}\bigg|_t \quad (16)$$

$$\eta^k(t+1) = \eta^k(t) - \theta \frac{\partial E^P}{\partial \eta^k}\bigg|_t \quad (17)$$

Work in this area focused on digital cameras. Characteristics that distinguish the camera model is based on the difference between process and technology components in a draw. For example, because the type of the lens, the size of the image sensor, CFA selection algorithm and the corresponding demosaicing processing algorithms, and the color image can be analysed to detect and quantify the characteristics of the optical distortion. The disadvantage of this method, in general, there are many models of components and a number of manufacturers and brands used in the process steps /algorithm to maintain the same or very similar between the different vehicle brand. Therefore, to reliably identify the source of the camera depends on the model relies on the model and the characterization of the following brief description of the various functions.

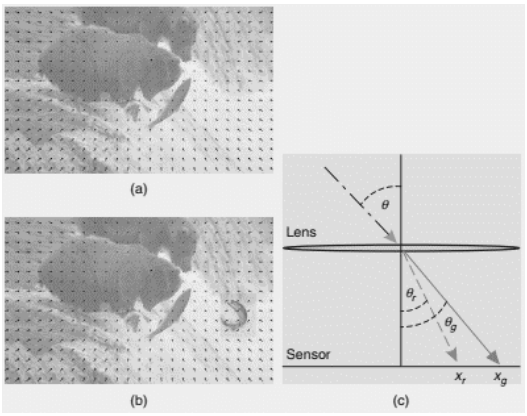

Figure 2. (a) Superimposed on the original image is a vector field. (b) The fish, taken from another image, was added to this image. (c) Polychromatic light enters the lens at an angle u and emerges at an angle that depends on wavelength.

Any forensic analysis of the first rule is definitely "the preservation of evidence." In this sense, the system lossy image compression such as JPEG forensic analysis can be considered as the greatest enemy. It is ironic, therefore, the loss of the unique properties of compression can be used for forensic analysis. Describes the detection of tampering compressed image three forensic techniques, a clear advantage of every detail lossy JPEG compression scheme. At least, any digital processing needs to be loaded into the software photo editing and re-save the image. Like most of the images are stored in JPEG format, it is possible that the original and the image processing are stored in that format. In this case, the compressed image is manipulated twice. Since the lossy nature of the JPEG image format, this dual oppression introduce compressed image does not exist in the individual special piece (assuming the second image is not compressed before they might). The presence of these devices, which can be used for any operation proof. Note that JPEG compression does not necessarily prove the double malicious tampering.

V.DETECTION OFJPEG COMPRESSION IN THEPRESENCE OFANTI-FORENSICS

The above analysis shows that it is possible to determine the anti-forensic image hesitate to check if the input noise is then quantified eliminated. Unfortunately, in practice, we do not have to re-quantization after the calculation of the mean square error distortion obtain the original JPEG compressed images. However, it can be observed that the blind can be used to detect the noise measurement in the presence of the dither signal in the spatial domain. Recalling For this purpose, any measure can be used to securely measure the amount of noise present in the image.

Hereinafter, the total amount of change (TV) measurement, which is defined as the norm of the image of the first order spatial derivative is used. The overall variation is due to noise is small, frequent changes in the pixel value corresponding to the edge is more sensitive to the sudden changes. Therefore, it is widely used as part of the optimization algorithm is a function of the target image noise removal. Of course, other metrics may also be used successfully. The show, for example, you can use the vector function SPAM average. In fact, its value is proportional to the noise in an image in an amount, which measures the strength of the correlation between the pixels.

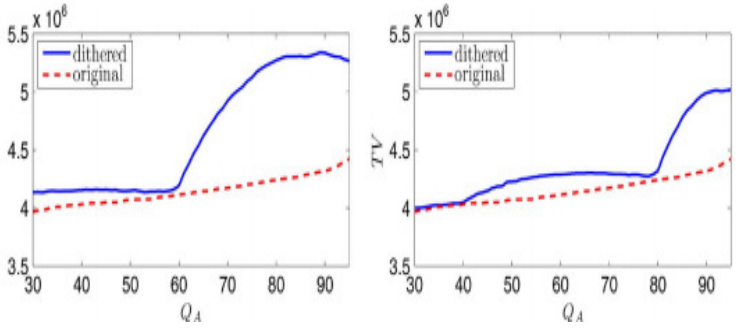

Figure 3. Jpeg compression anti-forensics.

In the following, we consider two cases. One of the following three conditions are discussed in Section IV-B, we assume that the original is available JPEG encoding on a priori knowledge, for example, belongs to a family of the initial quantization matrix corresponding to the matrix (such as the application IJG) quantization certain JPEG applications. In this configuration, the forensic analysis of a problem can be compressed using the same quantization matrix image as the original template.

VI.EXPERIMENTAL RESULTS

Consider creating a fake show two movie stars, is rumoured to be romantically involved walking along the beach at sunset. Personal image This image can be spliced together to establish for each actor. In doing so, it is generally difficult to accurately match lighting effects, wherein each individual original shoot. Introduce three methods to estimate the lighting environment, he was photographed several attributes of a person or object. By differences in light of the image can then be used as evidence of tampering. The general direction of the estimated source problem has been studied extensively in the field of computer vision (for example, [8,2,6]). In this section, the general problem is that, a standard solution, and then display the additional problem of how to simplify the management easier. We then extend this solution to provide a more effective and widely used forensic tools. Standard methods were used to estimate the light source direction beginning some simplifying assumptions: (1) the surface of interest is a isotropic light reflecting surface; (2) has a constant value of surface reflectivity; (3) Surface irradiated by a point source of light at infinity; direction and range of angles (4) of the normal to the surface and the light is from between 1 to 90◦.

(a) (b)

Figure 3. (a) An original image depicting two ladies with mountain scenery as background, (b) The two ladies have been hidden by background duplication

Some techniques used watermarking scheme verified image, and determining its integrity. Disadvantages associated with the watermark-based schemes is that the possibility that the watermark should be embedded in an imaging period of the right image and brand counterfeiting preventing water. It is practically difficult, because most of the digital cameras and other image capture device is not the device for instantaneous water marks. A group of 300 different images on the results given in Table 1 show that the repeated region also affects the size of the JPEG compression and the detection of noise to add an image rate. The area and / or higher quality JPEG higher SNR or larger size and better duplicate detection. However, this algorithm is repeated in a variety of sizes unmodified region accuracy rate of 100%.

Table 1: Results over a set of 300 images.

State of the image		Percentage Average detection over various sizes (pixels) of the duplicated regions		
Unprocessed duplication		16x16 region	64x64 region	128x128 region
JPEG Quality	100 95 80 70	100 98 50 5 1	100 98 98 60 50	100 100 100 98 70
SNR (db)	32 24	60 10	70 60	98 98

Finally, we compare the results with existing algorithms, as shown in Table 2, taking an image and the 8x8 block is 256 × 256. Table 2 shows our intent, that is, by a factor of four countries, while maintaining the application of principal component analysis in order to reduce the law. The complexity of the algorithm. In the method one substitution in the introduction which is more similar to SVD is conditional PCA, we want to promote the use of our algorithm unconditional PCA

(d) (ε)

Figure 4. (a) An image with a duplication, (b) The result of the proposed algorithm run on the Green channel of the image, accurately detecting the duplication.

VII.CONCLUSION

Fraud often involves creating a digital image synthesis from a single object / person. By doing so, difficult accurate lighting effects to match, due to the lighting direction (for example, in a clear day, the sun). At least one reason for this is that this manipulation may be required to create shadows and lighting gradient or destroyed. Although large irradiation direction can be quite obvious inconsistency, there is physical evidence of human psychology literature is the difference between human subjects surprisingly insensitive to the whole image of the lighting. The current technology allows to change and manipulate digital media, it is impossible only in the way 20 years ago. This proposed method based on ANN mechanism shows optimization approach for analyse the forgery images. As technology continues to evolve, it will become the science of computer forensics and more important, trying to keep up. Undoubtedly, as we continue the development of photographic techniques to expose fraud, new technology development, in order to make better fakes are difficult to detect. Some forensic tools can be more easily fooled will be more difficult than some of the other tools, for ordinary users to circumvent. For example, in the event of interference, in that the color filter array interpolation can simply reproduce the original lattice and the image of each color channel re interpolating. In addition, the amendment is inconsistent lighting is an extraordinary photo editing software program standards. Because spam / virus and anti-spam / virus in the game, the arms race between fake and forensic analyst inevitable. Forensic science field imaging, however, has and will continue for longer, more difficult (but not impossible) to create a forgery cannot be detected.

REFERENCES

[1] Lukáš, J., Fridrich, J., &Goljan, M. (2006, February). Detecting digital image forgeries using sensor pattern noise. In Electronic Imaging 2006 (pp. 60720Y-60720Y). International Society for Optics and Photonics.

[2] Ye, S., Sun, Q., & Chang, E. C. (2007, July). Detecting digital image forgeries by measuring inconsistencies of blocking artifact. In Multimedia and Expo, 2007 IEEE International Conference on (pp. 12-15). IEEE.

[3] Fridrich, A. J., Soukal, B. D., &Lukáš, A. J. (2003). Detection of copy-move forgery in digital images. In in Proceedings of Digital Forensic Research Workshop.

[4] Luo, W., Huang, J., &Qiu, G. (2006, August). Robust detection of region-duplication forgery in digital image. In Pattern Recognition, 2006. ICPR 2006. 18th International Conference on (Vol. 4, pp. 746-749). IEEE.

[5] Popescu, A. C., &Farid, H. (2004). Exposing digital forgeries by detecting duplicated image regions. Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515.

[6] Popescu, A. C., &Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. Signal Processing, IEEE Transactions on, 53(10), 3948-3959.

[7] Huang, H., Guo, W., & Zhang, Y. (2008, December). Detection of copy-move forgery in digital images using SIFT algorithm. In Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on (Vol. 2, pp. 272-276). IEEE.

[8] Popescu, A. C., &Farid, H. (2005). Exposing digital forgeries by detecting traces of resampling. Signal Processing, IEEE Transactions on, 53(2), 758-767.

[9] Kakar, P., Sudha, N., &Ser, W. (2011). Exposing digital image forgeries by detecting discrepancies in motion blur. Multimedia, IEEE Transactions on,13(3), 443-452.

[10] Farid, H. (2009). Exposing digital forgeries from JPEG ghosts. Information Forensics and Security, IEEE Transactions on, 4(1), 154-160.

[11] Gloe, T., Kirchner, M., Winkler, A., &Böhme, R. (2007, September). Can we trust digital image forensics?. In Proceedings of the 15th international conference on Multimedia (pp. 78-86). ACM.

[12] Farid, H. (2009). Image forgery detection. Signal Processing Magazine, IEEE,26(2), 16-25.

[13] Shivakumar, B. L., &SanthoshBaboo, L. D. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. Global Journal of Computer Science and Technology, 10(7).

[14] Johnson, M. K., &Farid, H. (2005, August). Exposing digital forgeries by detecting inconsistencies in lighting. In Proceedings of the 7th workshop on Multimedia and security (pp. 1-10). ACM.
[15] Cheddad, A., Condell, J., Curran, K., &McKevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal processing,90(3), 727-752.
[16] Sencar, H. T., &Memon, N. (2008). Overview of state-of-the-art in digital image forensics. Algorithms, Architectures and Information Systems Security, 3, 325-348.
[17] Zhang, C., & Zhang, H. (2007, December). Detecting digital image forgeries through weighted local entropy. In Signal Processing and Information Technology, 2007 IEEE International Symposium on (pp. 62-67). IEEE.
[18] Wolfgang, R. B., &Delp, E. J. (1996, September). A watermark for digital images. In Image Processing, 1996. Proceedings., International Conference on(Vol. 3, pp. 219-222). IEEE.
[19] Li, G., Wu, Q., Tu, D., & Sun, S. (2007). A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. InMultimedia and Expo, 2007 IEEE International Conference on (pp. 1750-1753).
[20] Gopi, E. S., Lakshmanan, N., Gokul, T., KumaraGanesh, S., & Shah, P. R. (2006, May). Digital image forgery detection using artificial neural network and auto regressive coefficients. In Electrical and Computer Engineering, 2006. CCECE'06. Canadian Conference on (pp. 194-197). IEEE.

Author

Muthu Kumar was born in Tirunelveli, India in 1989. He completed his Bachelor of Information and Technology in 2011. He completed his Master of Information and Technology in PSN College of Engineering in 2014. He currently working as assistant professor in PSN Engineering College in Department of computer science. He is a member of IEE Journals & Journal of the National Cancer Institute. He participated in many international conferences in various states and he published various International Journals related to brain tumor image Computing. His research interests primarily focus on image processing, especially in the methods related to biomedical image computing and processing through segmentation and classificaton, Robotic Surgery and Hologram.