ROW LEVEL IMAGE FORGERY DETECTION TECHNIQUE USING EMBEDDED DIGITAL SIGNATURES

Sahib Khan[1], Muneeza Wahid[2], Muhammad Abeer Irfan[1], Muhammad Naeem[3], Asma Gul[4], Muhammad Haseeb Zafar[2]

ABSTRACT

Image forgery detection is one of the most important issues in today's modern world. It has become very easy to change the contents of digital images with image editing tools and software. This paper is presenting a new technique to detect any changes made in digital images. This technique ensures the integrity of digital image at row level and using embedded digital signatures. Using message digest 5 algorithm, digital signature is generated from selected pixels of each row using selected pixels for and embedded in the least significant bits of selected pixel of the corresponding row of digital image. The proposed technique is powerful enough to detect different image manipulations. The results show that it can successfully detect one least significant bit alteration made in any pixel of digital image.

KEYWORDS: *Message digest five, Forgery detection, Watermarking, LSB substitution, RLIFD*

INTRODUCTION

Forgeries are the most important problems of today's modern of fast communication. These problems are not new to human; the traces can be found in ancient history and is considered as one of old problems. In the ancient era, it was specific to art and literature, but the public were safe from its harm. In modern of age of fast computer, the advancement of digital image processors, development of advance software and large number editing tools, an image can easily be manipulated and changed (Blythe *et al*., 2004). The changes and variations are difficult to detect visually, with naked eye, for human. The distinction between original and altered images, for human visual system (HVS) is almost impossible. The trend of forgeries is increasing in physical media, electronic media, social media and over the Internet rapidly (Khan *et al*., 2017). This tendency points out severe vulnerabilities and decreases the integrity of digital images.

Therefore, there is need of developing such techniques that authenticate digital images. This is very important to classify the forged and original images. To ensure integrity and prove the authenticity of the digital images become important, when images are presented as evidence in court of law, as intelligence substance, as a medical report, or as monetary credentials. In this sense, image forgery recognition is one of the most important aims of image forensics (Cox *et al*., 2001).

There are two major classes of forgery detection techniques, active techniques and passive techniques (Birajdar *et al*., 2013). Both the active and passive approaches have their own importance. In the active image forgery detection techniques pre-process digital image and extra information called watermarks are embedded in images, the watermark or signature are used as a source of authentication and integrity verification in digital images, but, this limit the application in practice (Gaborini *et al*., 2014). While, passive techniques, unlike, to active approach do not use any watermark or signature. Passive image forgery detection techniques roughly can be divided into five categories detail is available in (Redi *et al*., 2011). The passive forgery detection techniques make use of sensor pattern noise (SPN), fixed pattern noise (FPN) and photo response non-uniformity (PRNU). The PRNU is considered as the most reliable because of its multiplicative nature and it is unique for each individual image acquisition sensor (Chierchia *et al*., 2014).

In this paper a new image forgery detection technique is proposed. It processes digital image row by row and calculate digital signature for selected pixels each row using message digest five (MD5) algorithm (Deepakumara *et al*., 2001). In addition, the digital signature is hidden in least significant bits (LSB) of the remaining pixels, not used in the signature calculation, using four least significant bits (4LSB) substitution (Khan *et al*., 2016a; Khan *et al*., 2016b; Irfan *et al*., 2014). The basic reason of using MD5 algorithm is that it produces signature of fixed size i.e. 128 bits from variable input information. It

1 Department of Electronics and Telecommunications, Politecnico di Torino, Torino, Italy
2 Dept. of Electrical Engineering, University of Engineering and Technology Peshawar, Pakistan
3 Department of Computer Science, University of Peshawar, Pakistan
4 Department of Statistics, Shaheed Benazir Bhutto Women University Peshawar

is very easy to hide the 128 bits signature in 32 pixels, 4bits per pixel, using 4LSB substitution.

After a brief introduction, the remaining paper is organized in the following way. The section RLIFD technique, explains the detail implementation of the proposed technique, experimental results and discussion are presented in the section experimental results and analysis, followed by a section presenting comparison of the proposed technique with other state of the art techniques and last section finally concludes the paper.

RLIFD TECHNIIQUE

To detect the changes made in images various techniques are used, the detail is given in (Irfan *et al*., 2014; Lyu and Farid, 2002; Shi *et al*., 2005; Zou *et al*., 2006; Rad and wong, 2015; Kashyap *et al*., 2016). This research work focuses on a new active image forgery detection technique using digital signatures embedded in selected part of the same image. For digital signature calculation, MD5 algorithm is used.

The MD5 algorithm generates 128 bits signature and then 4LSB substitution is used to hide the signatures in the LSB of selected pixels. As 4 bits per pixel will be hidden so the 128 bits signature will need 32 pixels for their embedding.

To implement the proposed technique, each row of the image under process is divided in two parts. One part contains all the pixels used for signature calculation and are feed to MD5 algorithm as input. While, the other part contains pixel used for signature embedding using 4LSB substitution. Let the number of pixels in each row is “m”, then “m-32” pixels of each row are part of signature calculation group and 32 pixels are placed in embedding group. This portioning is shown in Figure 1. The MD5 algorithms process these “m-32” pixels and generate 128 bits digital signature for each row.

The 128 bits signature is hidden in the 32 pixels of the corresponding row. 4LSB substitution hide 4 bits per pixel in the and hence 32 pixels of each row successfully accommodates the 128 bits signature inside it. Let us consider that the image is of size “nxm”, where “n” is the number of rows and “m” is the number of columns. Therefore, each row will have “m” number of pixels. To detect forgery in whole image, signatures are calculated for all rows and hence MD5 algorithm ins applied “n” times and “n” digital signatures are calculated. To hide these signature 32 pixels per signature are needed. So, a total of “nx32” pixels out of “nxm” pixels are processed using 4LSB substitution. A total of “n” signature calculation and “nx32” substitution operations are performed to process a complete image of size “nxm”, using the proposed techniques.

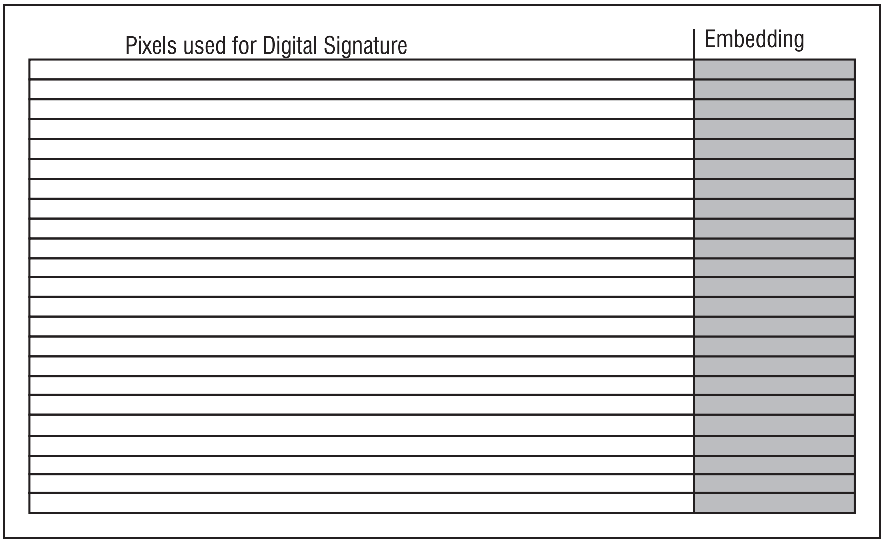


Figure 1: Row wise classification of pixels in signature and embedding pixels.

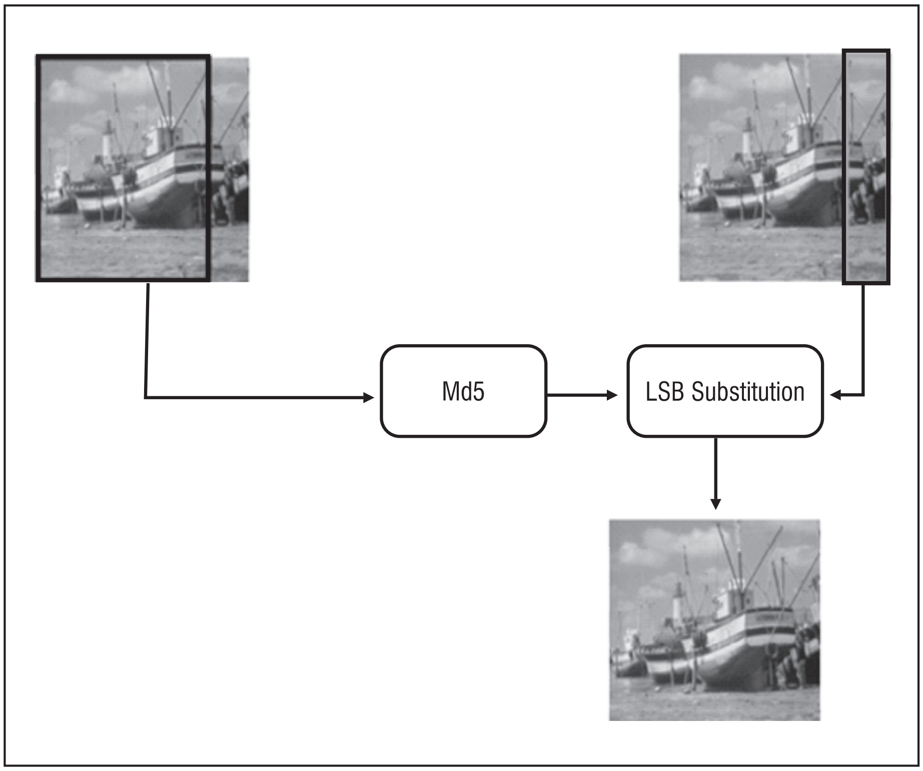


Figure 2: Flow chart diagram of Row level forgery detection at source side.

To further, elaborate the process, focus on the Figure 2. This shows the implementation of proposed technique with the help of block diagram. As shown the image under process is an array of pixels arrange with rows and columns. The image elements are classified in signature calculation part and signature embedding part as shown in Figure 2 with rectangle of black color and orange color respectively. The pixels of the signature part are given as input to MD5 algorithm row by row. MD5 algorithm generates 128 bits signature for each row, which is further feed to 4LSB substitution block for embedding and pixels of the signature embedding part are also feed to 4LSB substitution block. The 128 bits signature of the first row is embedded in 32 pixels of the first row and signature of second row is embedded in the 32 pixels of the second row and so on, until the whole image is processed. The whole process results in a final image with hidden digital signatures inside it. This final image is now ready to transmit, share or save on any media. If any manipulation is made in this image after being processed, the proposed technique is capable to detect the alteration.

After transmitting, sharing or storing the processed image, the main task is to check whether it is forged or not in the any stage in the meanwhile. Let suppose the image is transmitted and the receiver want to verify its integrity at receiver end. At the receiver end the received image pixels are again divided in two parts. The signature recalculation part and part of pixels with embedded signatures. The recalculation pixels are fee to MD5 row by row and digital signature is generated for each row. And pixels of the other part are processed using 4LSB retrieval. The MD5 generates 128 bits signature for each row and 4LSB retrieval, retrieve the 128 bits signature embedded at sender end. To detect any possible forgery in any row both signatures are compared with each other. If both the signatures are equal, then no forgery is detected, and the image is the same as transmitted. It ensures its integrity. In case, signatures do not match for any row, shows that the row is tempered. And the row is pointed out as forged one and hence forgery is detected. The whole process is shown in Figure 3.

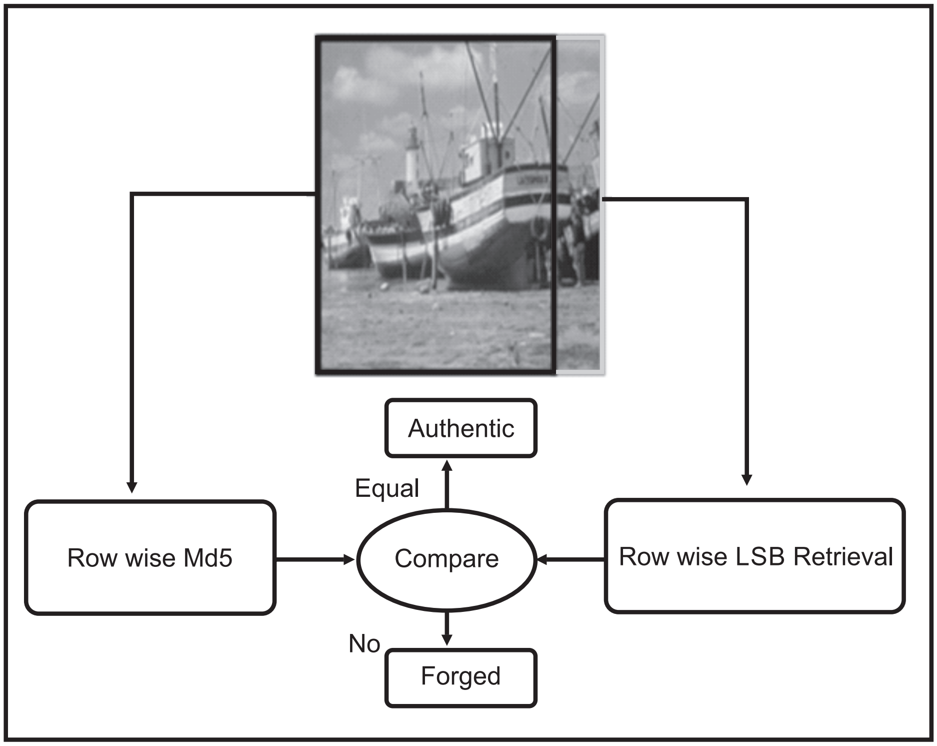


Figure 3: Forgery detection at receiver side

EXPERIMENTAL RESULTS AND ANALYSIS

Forgery is detected using row level image forgery detection techniques. The proposed technique is applied to image shown in Figure 4 (a). The image, in Figure 4 (a), is processed first to calculate digital signatures and embed the signature in selected pixels row wise. The resulted image with embedded signature is shown in Figure 4 (b).

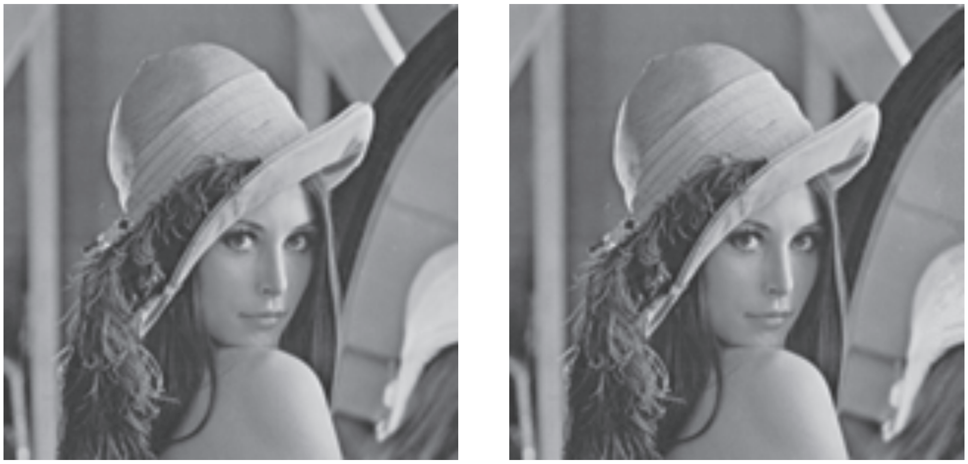

(a) (b)

Figure 4: Lena image a) Original image, b) Image with embedded digital signatures.

To check the strength of the proposed algorithm, the image in Figure 4(a) is manipulated in different manners. The manipulated images are shown in Figure 5(a, b, c, d and e). Figure 5(a), shows image manipulated by changing different pixels in different rows of image in Figure 4. Figure 5(b), presents the image with single pixel forgery in different rows. Figure 5(c), shows the truncated image, Figure 5(d), shows the manipulated image, in this image, multiple bits of a single pixels are altered and Figure 5(e) presents image with only LSB forged in a single pixel.

These manipulated images are then passed through row level image forgery detection method. The experimental results show that proposed technique successfully detects all types' manipulation and changes made in the images. It points out the row in which manipulation is made. All the forged rows are labeled as shown in Figure 6. Here is the row with forgeries are replaced by black pixels i.e. all the pixels are set to zero by the proposed algorithm. While, all unaffected rows are not changed, representing the authenticity of the pixels of the rows.

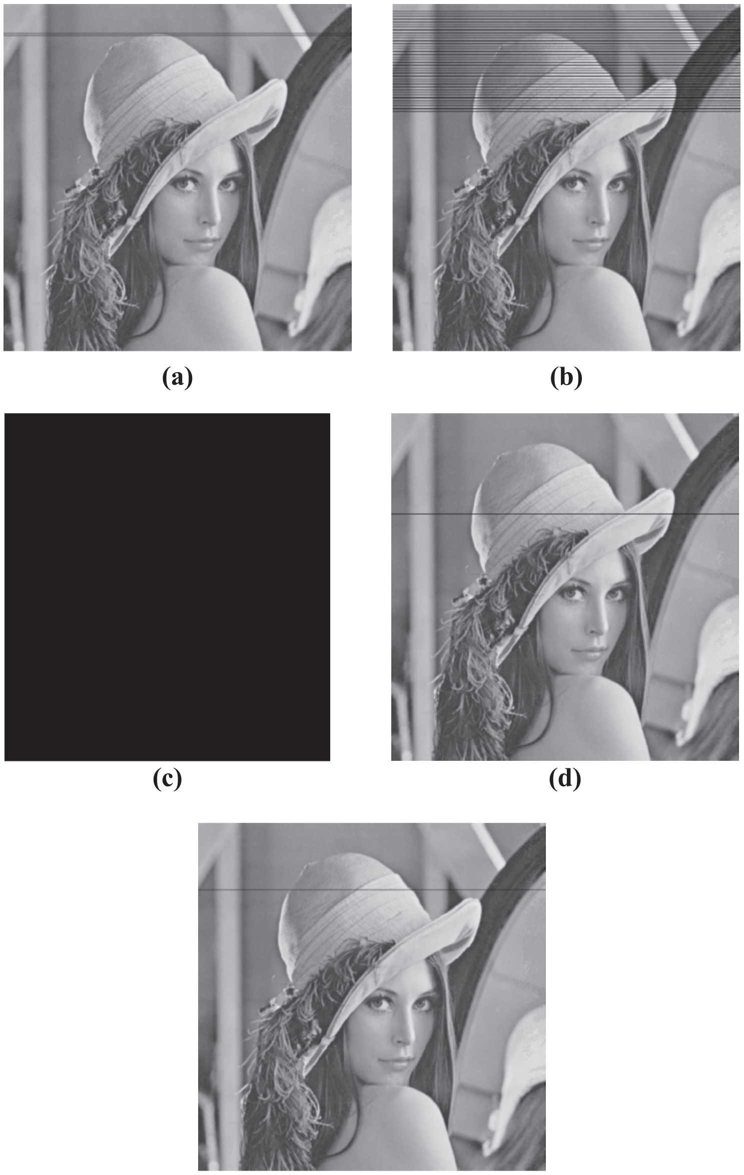
(a) **(b)**

(c) **(d)**

(e)

Figure 5: Forged images a) altered image with changes in various pixels of different rows, b) Single pixel forgery in different rows, c) Truncated image, d) multiples bits forged in a single pixel, e) One LSB forged in single pixel.

To further verify and strengthen the claim of the work. The proposed technique is applied on a set image forged with rows manipulation, rows truncation, columns truncation, single row alteration, multiple bits manipulation, blurring, high pass filtering, rotating, and one LSB manipulation. Set of images contain 10% of each type of forged images. While, 10% images set is composed of unaltered the images. The result shows that the proposed technique successfully classified all the images as forged and original images, except row truncation. The proposed algorithm fails to detect row elimination i.e. row truncation, in an image. Therefore, the only limitation of this technique is to detect row truncation.



(a)

(b)

(c)

(d)

(e)

Figure 6: Forgery detected images a) Alteration detected in multiple pixels in different rows, b) changes detected in different pixels in a single row, c) Truncation detection, d) Different bits manipulation in one pixel detected, e) One LSB manipulation in one pixel detected.

COMPARISON

In this section, comparison of proposed method with other state of the art techniques is presented. The comparison is made in term of true positive (TP), true negative (TN) and accuracy. The values listed in Table 1, demonstrates the comparison of the proposed techniques with Lyu and Farids, 2002; Shi *et al.*, 2005; Zou *et al*., 2006; Rad and Wong, 2015; and Kashyap *et al*., 2016; methods.

The results show that among all the previous techniques mentioned in Table 1, Kashyap *et al*., 2016; technique has the highest detection accuracy of 81.50%. While the proposed technique demonstrated detection accuracy equal to 95%. Therefore, proposed method is a more powerful technique, to detect manipulations in digital images.

Table 1: Comparison with previous techniques

Sr. No.	Technique	TP (%)	TN (%)	Accuracy (%)
1	Lyu and Farids	78.20	69.39	73.75
2	Shi et al.	75.55	76.02	75.78
3	Zou et al.	77.40	75.07	76.21
4	Rad et al.	80.11	77.61	78.80
5	Kashyaop et al.	83.33	76.0	81.50
6	Proposed Technique	96.51	95.78	95.01

CONCLUSION

Row level image forgery detection technique is a powerful method to identify various types of manipulation, including rotation, truncation, and single or multiple pixels alteration in digital images. The technique uses hidden digital signatures to identify the forged row or rows. It has been proved by the experimental results that it can identify the forged row or rows with significant accuracy, even if a single bit is changed. The exquisiteness of the technique is that the existence of the hidden signatures remains innocent and do not attract HVS. In conclusion, RLIFD technique can easily authenticate digital image contents and locate the affected row or rows.

REFERENCES

1. *Birajdar, G. K., and Mankar, V. H., (2013), "Digital image forgery detection using passive techniques: A survey", Digital Investigation, Vol. 10, No. 3, pp. 226-245.*

2. *Blythe, P., and Fridrich, P., (2004), "Secure digital camera", In Proceedings of Digital Forensic Research Workshop, Baltimore, MD, pp. 11-13.*

3. *Chierchia, G., Poggi, G., Sansone, C., and Verdoliva, L., (2014), "A Bayesian-MRF approach for PRNU-based image forgery detection", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 4, pp. 554-567.*

4. *Cox, I., Miller, M. L., and Bloom, J. A., (2001), "Digital Watermarking", San Matteo, CA: Morgan Kaufmann.*

5. *Deepakumara, J., Heys, H. M., and Venkatesan, R., (2001), "FPGA implementation of MD5 hash algorithm", In Canadian Conference on Electrical and Computer Engineering, Vol. 2, pp. 919-924.*

6. *Gaborini, L., Bestagini, P., Milani, S., Tagliasacchi, M., and Tubaro, S., (2014), "Multi-clue image tampering localization", In IEEE International Workshop on Information Forensics and Security (WIFS), pp. 125-130.*

7. *Irfan, M. A., Ahmad, N. and Khan, S., (2014), "Analysis of varying least significant bits DCT and spatial domain stegnography", Sindh University Research Journal-SURJ (Science Series), Vol. 46, No. 3, pp. 301-306.*

8. *Kashyap, A., Parmar, R. S., Suresh, B., Agarwal, M., and Gupta, H., (2016), "Detection of digital image forgery using wavelet decomposition and outline analysis", In International Conference on Signal Processing and Communication (ICSC), pp. 187-190.*

9. *Khan, S., Ahmad, N., and Wahid, M., (2016a) "Varying index varying bits substitution algorithm for the implementation of VLSB steganography", Journal of the Chinese Institute of Engineers, Vol. 39, No. 1, pp. 101-109.*

10. *Khan, S., Ismail, M., Khan, T., and Ahmad,*

N. (2016b), "Enhanced stego block chaining (ESBC) for low bandwidth channel", Security and Communication Networks, Vol. 9, No. 18, pp. 6239-6247.

11. *Khan, S., Naeem, M., Khan, T., and Ahmad, N., (2017), "4LSB based data hiding in complex region of digital images and its effects on edges and histogram", Journal of Engineering and Applied Sciences (JEAS), Peshawar, Vol. 36, No. 1, pp. 67-75.*

12. *Lyu, S., and Farid, H., (2002), "Detecting hidden messages using higher-order statistics and support vector machines", In Information Hiding, pp. 340-354.*

13. *Rad, R. M., and Wong, K., (2015), "Digital image forgery detection by edge analysis", In IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), pp. 19-20.*

14. *Redi, J. A., Taktak, W., and Dugelay, J. L., (2011), "Digital image forensics: A booklet for beginners", Multimedia Tool Application, Vol. 51, No. 1, pp.133-162.*

15. *Shi, Y. Q., Xuan, G., Zou, D., Gao, J., and Yang C., (2005), "Steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network", In International Conference on Multimedia and Expo, Amsterdam, Netherlands, pp. 269-272.*

16. *Zou, D., Shi, Y. Q., Su, W., and Xuan, G., (2006), "Steganalysis based on Markov model of thresholded prediction-error image", In IEEE International Conference on Multimedia and Expo, pp. 1365-1368.*