# Nonintrusive Image Tamper Detection Based on Fuzzy Fusion

**Girija Chetty[+] and Monica Singh[††],**

[+]Faculty of Information Sciences and Engineering,
University of Canberra, Australia
[††] Video Analytics Pty. Ltd.
Melbourne, Australia

**Summary**
In this paper, we propose a novel fuzzy fusion of image residue features for detecting tampering or forgery in video sequences. We suggest use of feature selection techniques in conjunction with fuzzy fusion approach to enhance the robustness of tamper detection methods. We examine different feature selection techniques, the independent component analysis (ICA), and the canonical correlation analysis (CCA) for achieving a more discriminate subspace for extracting tamper signatures from quantization and noise residue features. The evaluation of proposed fuzzy fusion technique along with different feature selection techniques for copy-move tampering emulated on low bandwidth Internet video sequences, show a significant improvement in tamper detection accuracy with fuzzy fusion.

***Key words:***
*image tampering, digital forensics, feature selection, fuzzy fusion.*

## 1. Introduction

Digital Image tampering or forgery has become major problem lately, due to ease of artificially synthesizing photographic fakes- for promoting a story by media channels and social networking websites. This is due to significant advances in computer graphics and animation technologies, and availability of low cost off-the-shelf digital image manipulation and cloning tools. With lack of proper regulatory frameworks and infrastructure for prosecution of such evolving cyber-crimes, there is an increasing dissatisfaction about increasing use of such tools for law enforcement, and a feeling of cynicism and mistrust among the civilian operating environments.

Another problem this has lead to, is a slow diffusion of otherwise extremely efficient image based surveillance and identity authentication technologies in real-world civilian operating scenarios. In this paper we propose a novel information fusion based formulation for detecting image tampering and forgery. The proposed technique involves extraction of noise and quantization residue features from intra-frame and inter-frame pixel sub-blocks from video sequences, their transformation into discriminant subspace (ICA, CCA) and subsequent fusion based on fuzzy integral. The proposed fuzzy fusion based formulation allow detecting the tamper or forgery in low-bandwidth video (Internet streaming videos), using blind and passive tamper detection techniques and attempts to model the source signatures embedded in camera pre-processing chain. By sliding segmentation of image frames, we extract intra-frame and inter-frame pixel sub-block residue features, transform them into optimal cross-modal subspace, and perform multimodal fusion to detect evolving image tampering attacks, such as JPEG double compression, re-sampling and retouching. The promising results presented here can result in the development of digital image forensic tools, which can help investigate and solve evolving cyber crimes.

## 2. Background

Digital image tamper detection can use either active tamper detection techniques or passive tamper detection techniques. A significant body of work, however, is available on active tamper detection techniques, which involves embedding a digital watermark into the images when the images are captured. The problem with active tamper detection techniques is that, not all camera manufacturers embed the watermarks, and in general, most of the customers have a dislike towards cameras which embed watermarks due to compromise in the image quality and the intrusive nature of the approach. So there is a need for passive, non-intrusive and blind tamper detection techniques with no watermarking in the images.

Non-intrusive, passive and blind image tamper detection is a relatively new area and recently some methods have been proposed in this area. Mainly these are of two categories [1, 2, 3, 4]. Fridrich [4] proposed a method based on hardware aspects, using the feature extracted from photos. This feature called sensor pattern noise is due to the hardware defects in cameras, and the tamper detection technique using this method resulted in an accuracy of 83% accuracy. Chang [5] proposed a method based on camera response function (CRF), resulting in detection accuracy of 87%, at a false acceptance rate (FAR) of 15.58%. Chen et al. [6] proposed an approach for image tamper detection based on a natural image model, effective in detecting the change of

Manuscript received September 5, 2010
Manuscript revised September 20, 2010

correlation between image pixels, achieving an accuracy of 82%. Gou et al [7] introduced a new set of higher order statistical features to determine if a digital image has been tampered, and reported an accuracy of 71.48%. Ng and Chang [8] proposed bi-coherence features for detecting image splicing. This method works by detecting the presence of abrupt discontinuities of the features and obtains an accuracy of 80%. Popescu and Farid [3] proposed different CFA (colour filter array) interpolation algorithms within an image, reporting an accuracy of 95.71% when using a 5x5 interpolation kernel for two different cameras. A more complex type of passive tamper detection technique, known as "copy-move tampering" was investigated by Bayram, Sencar, Dink and Memon [1,2] by using low cost digital media editing tools such as Cloning in Photoshop. This technique usually involves covering an unwanted scene in the image, by copying another scene from the same image, and pasting it onto the unwanted region. Further, the tamperer can use retouching tools, add noise, or compress the resulting image to make it look genuine and authentic. Finally, detecting tampers based on example-based texture synthesis scheme was proposed by Criminisi et al[9] that is based on filling in a region from sample textures. It is one of the state-of-the-art image impainting or tampering schemes. Gopi et al in [10] proposed a pattern recognition formulation and used auto regression coefficients and neural network classifier for tamper detection

One of the objectives of the work reported here is development of robust and automatic tamper detection framework for low bandwidth Internet streamed videos where most of the fingerprints left by tamperer can get perturbed by heavy compression used for reducing the bandwidth. However, by fusing multiple image tampering detectors, it could be possible to uncover the tampering in spite of the heavy compression, as different detectors use cues and artifacts at different stages of the image formation process. So if an image lacks certain cues, a complementary detector would be used for making a decision For example, a copy move forgery might have been created with two source images of similar quantization settings but very different cameras. In this case, the copy move forgery can be successfully detected by a different detector. We thus benefit from having several tamper detection modules at hand rather than only using the one type of detector. Another advantage of fusing several detector outputs to make a final decision is that, if one of the detector outputs noisy and erroneous scores, the other detectors could complement and enhance the reliability of the tamper decision. Therefore, the advantage of fusion is twofold: to handle images which were subjected to multiple, diverse types of tampering, and to boost the detection robustness and accuracy by making different modules work with each other. The challenge, however, lies in the synergistic fusion of diverse detectors as different detectors are based on different physical principles and segmentation structures.

We formulate the tamper detection problem in this paper using the pattern recognition framework, and fuzzy fusion technique to fuse different image features in the discriminant subspace (ICA and CCA) features. The approach involves several stages. The first stage involves extracting noise and quantization residue features from intra-frame and inter-frame pixel sub blocks (which we refer to hence forth in this paper as macro blocks). The next stage involves transformation of quantization and noise residue features into more discriminant subspace using different feature selection techniques such as the CCA or ICA analysis. Use of feature selection technique reduces the dimensionality of the features making it less computational intensive. Finally, by using a threshold based classifier (GMM or SVM), we localize the tamper zones in the images. To enhance the confidence level of each of the individual tamper detectors, we perform a fusion based on fuzzy integral. The complete approach is non-intusive, blind and passive and extends the noise residue features reported by Hsu et al in [11] and expands the pattern recognition formulation proposed by Gopi et al in [10]. The approach is based on the hypothesis, that typical tampering attacks such as double compression, re-sampling and retouching can inevitably disturb the correlation properties of the macro blocks within a frame (intra-frame) as well as between the frames (inter-frame) and can distinguish the fingerprints or signatures of genuine video from tampered video frames. The rest of the paper is organized as follows. Next Section describes the formulation of fusion problem. The details of the experimental results for the proposed fusion scheme are described in Section 4. The paper concludes in Section 5 with some conclusions and plan for further work.

## 3. Fuzzy Fusion Formulation

The processing pipeline once the images or video is captured consists of several stages. First, the camera sensor (CCD) captures the natural light passing through the optical system. Generally, in consumer digital cameras, every pixel is detected by a CCD detector, and then passed through different colour filters called Color Filter Array (CFA). Then, the missing pixels in each color planes are filled in by a CFA interpolation. Finally, operations such as demosaicing, enhancement and gamma correction are applied by the camera, and converted to a user-defined format, such as RAW, TIFF, and JPEG, and stored in the memory.

Since the knowledge about the source and exact processing (details of the camera) used is not available for application scenarios considered in this work (low-

bandwidth Internet video sequences), and which may not be authentic and already tampered, we extract a set of residual features for macro blocks within the frame and between adjacent frames from the video sequences. These residual features try to model and extract the fingerprints for source level post processing within any camera, such as denoising, quantization, interlacing, de-interlacing, compression, contrast enhancement, white balancing, image sharpening etc. In this work, we use only two types of residual features: noise residue features and quantization residue features.

The noise and quantization residue features were first extracted from 32 x 32 pixel intra-frame and inter-frame macro blocks of the video sequences. The details of noise and quantization residue features are described in [3], [4] and [11]. A feature selection algorithm was used to select those features that exhibit maximal significance. We used feature selection techniques based on three different techniques: Fisher linear discriminant analysis (FLD), canonical correlation Analysis (CCA), and Independent component analysis (ICA). The details of these feature selection techniques are described in [12], [13]. The fuzzy fusion scheme used to combine different features is described below:

- Once we compute ICA and CCA features, we vectorize the features (X) and normalize them prior to fusion. The normalized vector Λ of an original vector X is defined as:

$$\Lambda = \frac{\mathrm{X}}{\sqrt{(\mathrm{X}^{\mathrm{T}} X)}} \qquad (1)$$

- Then we fuzzify the inputs by mapping the normalized input vector (Λ) to values between 0 and 1, to represent the evidence that the object satisfies class hypothesis Ck. The membership function is then generated using a histogram based method [18], [19] and [20].

- If *x* represents the distance of input from its class, and if *h(x)* represents the histogram of x, we can construct membership function *u(x)* as:

$$u(x) = \int_{x}^{+\infty} h(x)dx. \qquad (2)$$

From Eqn(2), we can construct membership function for each input as shown below:

- If we represent a function $\xi_k = \|\Lambda - \Lambda_k\|$, where $\Lambda_k$ represents the vector describing the $k^{th}$ class. The result of fuzzification $S_k$ can be shown as:

$$S_k = u(\xi_k) \qquad (3)$$

- Fuzzy integral considers the objective evidence supplied by each input (represented by *h-function*) and expected worth of each input (via a fuzzy measure).

- If $x_1$ represents the input 1, and $x_2$ represents input 2, and if the fuzzy density value $g^i = g\{x_i\}$ is determined via statistical measurements on recognition rate of the single input $x_i$, the output of fuzzy integral $F_k$ can be expressed as:

$$F_k = \begin{cases} \max(\min(S_{kX_1}, g^1), S_{kX_2} & S_{kX_1} > S_{kX_2} \\ \max(\min(S_{kX_2}, g^2), S_{kX_1} & else \end{cases} \qquad (4)$$

Where $S_{kX_1}$, $S_{kX_2}$ are two fuzzified inputs.

- Finally. we classify the input into a specific class if that class if that class has maximum output of fuzzy integral

$$y = \arg\max_{k} F_k \qquad (5)$$

Figure 1 shows the block schematic for the fuzzy fusion scheme.

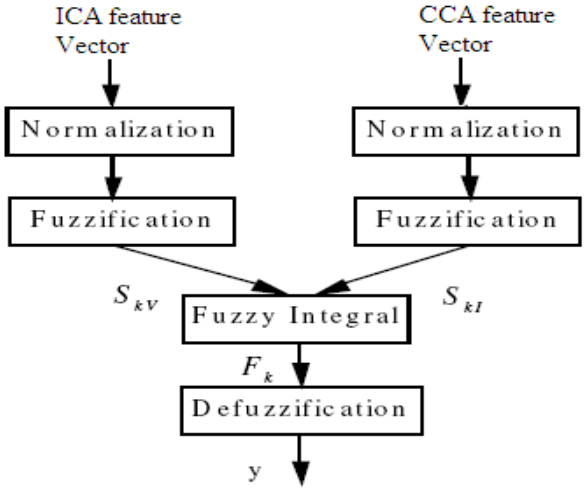


Fig. 1: Block schematic of the proposed fuzzy fusion scheme

## 4. Experimental Results

The video sequence data base from Internet movie sequences was collected and partitioned into separate subsets based on different actions and genres. The data collection protocol used was similar to the one described in [14]. Figure 2 shows screenshots corresponding to different actions, along with emulation of copy move tampered scenes and the detection of tampered regions with the proposed approach.

Fig. 2: Screenshots from Internet streamed video sequences; Row 2: Copy-move tamper emulation for the scene; Row 3: Detection of tampered regions in the scene

Different sets of experiments were conducted to evaluate the performance of the proposed feature selection approaches, namely, the ICA, \and the CCA and their fuzzy fusion in terms of tamper detection accuracy. The experiments involved a training phase and a test phase. In the training phase, a Gaussian Mixture Model for each video sequence from data base was constructed [15]. In the test phase, copy-move tamper attack was emulated by artificially tampering the training data. The tamper processing involved copy cut pastes of small regions in the images and hard to view affine artifacts. Two different types of tampers were examined. An intra-frame tamper, where the tampering occurs in some of the macro blocks within the same frame, and inter-frame tamper, where macro blocks from adjacent frames were used. However, in this paper, we present and discuss results for the intra-frame tamper scenario only. We compared the performance of proposed fuzzy fusion scheme with feature selection based on autoregressive coefficients and neural network based classification proposed by Gopi et al in [10].

As can be seen in Table 1, the single mode noise residue features perform better than quantization residue features. For both noise residue and quantization residue features, the CCA, and ICA features perform better than ARC features. CCA features result in better accuracy for noise residue features as compared to others, as they are based on canonical correlation analysis that can extract maximal correlation properties. However, for quantization residue features, the ICA features perform better than CCA features showing that quantization information perturbed by tampering may not be necessarily correlated, but could contain certain independent components. By fusing intra-frame and inter-frame macro block features by fuzzy fusion, we can see a better performance is achieved.

TABLE 1: EVALUATION OF NOISE AND QUANTIZATION RESIDUE FEATURES FOR EMULATED COPY-MOVE TAMPER ATTACK (% ACCURACY); $\tilde{f}_{Intra-Inter}$ ( NOISE RESIDUE FEATURES); $f_{Intra-Inter}$ ( QUANTIZATION RESIDUE FEATURES)

| Internet movie data subset | % Accuracy | | |
|---|---|---|---|
| Different Residue features and their fusion | CCA | ICA | ARC[10] |
| $f_{Intra}$ (Intra-frame noise residue features) | 83.2 | 83.4 | 80.2 |
| $f_{Inter}$ (Inter-frame noise residue features) | 83.8 | 83.1 | 83.1 |
| $\tilde{f}_{Intra}$ (Intra-frame quant. residue features) | 77.28 | 80.26 | 74.33 |
| $\tilde{f}_{Inter}$ (Inter-frame quant. residue features) | 72.65 | 78.27 | 69.45 |
| $f_{Intra-Inter}$ (feature fusion- noise residue) | 86.6 | 86.1 | 83.78 |
| $\tilde{f}_{Intra-Inter}$ feature fusion- quant residue) | 80.55 | 82.34 | 77.22 |
| $f_{Intra-Inter} + \tilde{f}_{Intra-Inter}$ (hybrid fusion) | 89.56 | 88.85 | 84.33 |

This shows that better correlation information can be extracted when multiple frames are used for detecting tampers. Further, by fusing the two detectors, the detectors based on noise residue features and quantization residue features, we can see that a better performance is achieved as the two detectors complement each other, resulting in a consistent and stable performance. This can be expected as quantization artifacts for low-bandwidth video can significant damage tamper related correlation properties. However, by using a hybrid fuzzy fusion of quantization and noise residue features from macro blocks, and using different feature selection techniques, we can see that a better performance is achieved (last row in Table 1).

## 5. Conclusions

In this paper, we propose a novel fuzzy fusion of image residue features for detecting tampering or forgery in video sequences. We suggest use of feature selection techniques in conjunction with fuzzy fusion approach to enhance the robustness of tamper detection methods. We examine different feature selection techniques, the independent component analysis (ICA), and the canonical correlation analysis (CCA) for achieving a more discriminate subspace for extracting tamper signatures from quantization and noise residue features. The evaluation of proposed fuzzy fusion technique along with different feature selection techniques for copy-move tampering emulated on low bandwidth Internet video sequences, show a significant improvement in tamper detection accuracy with fuzzy fusion.

## References

[1] Bayram S., Sencar H. T., and Memon N.,"An Efficient and Robust Method For Detecting Copy-Move Forgery". In Proceedings IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2009, Taipei Taiwan, June 2009.

[2] Dirik A. E., and Memon N., "Image Tamper Detection Based on Demosaicing Artifacts", Proceedings IEEE ICIP 09, November 2009, Cairo Egypt.

[3] Popescu A.C. and Farid H., "Exposing Digital Forgeries by Detecting Traces of Re-sampling",IEEE Transactions on signal processing ,Vol. 53,No.2,February 2005 .

[4] Fridrich J., Sukal David., and Lukas Jan, "Detection of Copy-Move Forgery in Digital Images", http://www.ws.binghamton.edu/fridrich/Research/copymove.pdf

[5] Hsu Y. F., and Chang S.F.. "Detecting Image Splicing Using Geometry Invariants and Camera Characteristics Consistency", In ICME, Toronto, Canada, July 2006.

[6] Shi Y. Q., Chen C., and Chen W., "A natural image model approach to splicing detection," in Proc. ACM Multimedia Security Workshop, pp. 51-62, Sept. 2007, Dallas, Texas.

[7] Gou H., Swaminathan A., and Wu M., "Noise Features for Image Tampering Detection and Steganalysis," Proc. of IEEE Int. Conf. On Image Processing (ICIP'07), San Antonio, TX, Sept. 2007.

[8] Ng T. T., Chang, C S. F.. Lin Y., and Sun Q., "Passive-blind Image Forensics", In Multimedia Security Technologies for Digital Rights, W. Zeng, H. Yu, and C. –Y. Lin (eds.), Elsvier, 2006.

[9] Criminisi A., Perez P, and Toyama K., "Region filling and object removal by exemplar-based image inpainting," IEEE Trans. Image Process., vol.13, no.9, pp. 1200-1212, Sept. 2004

[10] Gopi E.S.; Lakshmanan N.; Gokul T; KumaraGanesh S.; Shah P.R.; "Digital Image Forgery Detection using Artificial Neural Network and Auto Regressive Coefficients", Proceedings Canadian Conference on Electrical and Computer Engineering, 7-10 May 2006, Ottawa, Canada, pp. 194 – 197.

[11] Hsu C., Hung T., Lin C., Hsu C., "Video Forgery Detection Using Correlation of Noise Residues", retrieved on 11/3/2010. www.ee.nthu.edu.tw/~cwlin/pub/mmsp08forensics.pdf

[12] Martinez A. M., and Kak A. C., (2001). "PCA versus LDA". IEEE Transactions on Pattern Analysis and Machine Intelligence 23 (2): 228–233. doi:10.1109/34.908974. , retrieved on 11/3/2010. http://www.ece.osu.edu/~aleix/pami01.pdf.

[13] Borga M., and Knutsson H., "Finding Efficient Nonlinear Visual Operators using Canonical Correlation Analysis, " in Proc. of SSAB-2000, Halmstad, pp. 13-16.

[14] Laptev I., Marszałek M., Schmid C. and Rozenfeld B., "Learning realistic human actions from movies" (2008), in Proc. CVPR'08, Anchorage, USA.

[15] Chetty G. & Wagner M, "Robust face-voice based speaker identity verification using multilevel fusion" (2008), mage and Vision Computing Volume 26, Issue 9, 1 September 2008, Pages 1249-1260.

[16] Hyvarinen A., and Oja, E., 2000, "Independent Component Analysis: Algorithms and Applications", Neural Networks, 13(4-5):411-430, 2000.

[17] H. Farid and S. Lyu, "Higher-Order Wavelet Statistics and their Application to Digital Forensics," IEEE Workshop on Statistical Analysis in Computer Vision, Madison, WI, 2003.

[18] Zadeh, L. A.: Fuzzy sets. Information and Control 8 (1965) 338–353.

[19] Medasani, S., Kim, J., Krishnapuram, R.: An overview of Membership Function Generation Techniques for Patter Recognition. International Journal of Approximate Reasoning 19 (1998) 391–417

[20] Keller, J. M., Osborn, J.: Training the Fuzzy Integral. International Journal of Approximate Reasoning 15 (1996) 1–24.