THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 13 | Number 2 Article 8

October 2018

Enhancement of Media Splicing Detection: A General Framework

Songpon TEERAKANOK
Graduate School of Information Science and Engineering, Ritsumeikan University,
songpon.te@cysec.cs.ritsumei.ac.jp

Tetsutaro UEHARA
Department of Information Science and Engineering, Ritsumeikan University, uehara@cs.ritsumei.ac.jp

Recommended Citation

TEERAKANOK, Songpon and UEHARA, Tetsutaro (2018) "Enhancement of Media Splicing Detection: A General Framework," *Journal of Digital Forensics, Security and Law*: Vol. 13 : No. 2 , Article 8.
DOI: https://doi.org/10.15394/jdfsl.2018.1481
Available at: https://commons.erau.edu/jdfsl/vol13/iss2/8

ENHANCEMENT OF MEDIA SPLICING DETECTION: A GENERAL FRAMEWORK

No institute defined

ABSTRACT

Digital media (i.e. image, audio) has played an important role in today information system. The increasing of popularity in digital media has brought forth a number of technology advancements. This, however, also gives birth to a number of forgeries and attacks against this type of information. With the availability of easy-to-use media manipulating tools available online, the authenticity of today digital media cannot be guaranteed. In this paper, a new general framework for enhancing today media splicing detection has been proposed. By combining results from two traditional approaches, the enhanced detection results show improvement in term of clarity in which anomalies are more explicitly shown, providing easier and faster way for a forensic practitioner to investigate and verify the authenticity of the target digital media. Regarding the experiment, the developed framework is tested against a number of realistic tampered (spliced) media. Moreover, the enhanced detection results are compared with traditional approaches in order to ensure the efficiency of our proposed method in the realistic situation.

Keywords: splicing, forgery, digital forensics, similarity measurement, media tampering

1. INTRODUCTION

Media forgery has become one of the most critical issues in today digital information system. With helping of easy-to-use and also easy-to-access tools available online, a realistic tampered media (e.g. photo or video), leaving no trace that is detectable by human normal perceptions, can be forged in no time.

Regarding crime investigation, collecting and verifying of every evidence are crucial processes needed to be carefully performed. Moreover, in the court of law, the authenticity of every single digital evidence is utmost important. However, digital evidence, in many cases, cannot be trusted or judged by only human basic perceptions (e.g. naked eyes). Thus, digital forensic has come to tackle this problem.

There are several cases involving media forgery presented in press, including the Reuters's altering of a photo of bombing incident in Beirut (Lappin, 2006), duplicating of missile pictures in the photo of Iran's provocative missile tests appeared in Los Angeles Times, The Chicago Tribune and several major news website including BBC News and The New York Times (Nizza & J. Lyons, 2008) and, regarding digital audio, controversy over the authenticity of an audio clip claimed to be Osama Bin Laden's voice (A. Muller, 2004).

There are several ways to tamper a target digital media. Concerning digital images, image retouching (Sundaram.A & Nandini, 2015), splicing (Birajdar & Mankar, 2013) and copy-move forgery (CMF) (Al-Qershi & Khoo, 2013) are most common yet popular types of attack on digital image. Retouching, Cloning, and Healing are image manipulation methods in which parts of the target digital image are removed, concealed, blurred or emphasized by using parts or properties from the same image. This type of attack also includes adjusting of some image properties, e.g. brightness, contrast, color temperature and white balance.

Splicing is one of the most common and popular image manipulation technique involved in many crime cases. Regarding splicing, the general idea behind this kind of attack is to replace parts of the target digital image with image fragments from different sources of images. With image content from different sources, the forged image can lead to controversy, misunderstanding or misinterpretation. An interesting case of spliced image that can be found every day is Clickbait (Chakraborty, Paranjape, Kakarla, & Ganguly, 2016). Clickbait is a term referring to web content that is placed on the web page in order to attract users' attention and generating advertising revenue when a user click on the corresponded web content. The content of Clickbait normally rely on exploiting user's curiosity by using attractive headlines with eye-catching thumbnail pictures which, in most case, are tampered using splicing and CMF.

Copy-Move forgery (Warif et al., 2016) (or CMF, for short) is a type of attack in which some parts of the target image are duplicated and placed somewhere in the same digital image. CMF is mainly used to conceal or emphasized some parts of the target digital image. A good example of an image forgery using CMF is the picture of missile tests in Iran (show in figure 1) which the picture of missiles are duplicated in order to make the target digital image more frightful.

Figure 1: Tampered image of Iranian provocative missile tests.

Source: `https://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many`

There are also a number of attack on digital audio proposed in the literature. Similar to digital image forgery, splicing and CMF are also one of the most important types of attack on audio media. In splicing, some audio fragments from different sources are placed in target audio file in order to lead the audience to misunderstand or misinterpretation. This type of forgery is normally done with some audio post-processing process in order to make the forged audio more realistic and hardly or unnoticeable by human ears. The same goes for CMF, in which parts of target audio are duplicated and placed back to the same audio file in order to emphasize or conceal some audio information.

Concerning other types of audio forgery, deletion, a method where some parts of the audio signal are cut in order to get rid of unwanted information, is also a simple yet powerful manipulation method in which, if done properly, harder to detect compared to splicing or CMF.

Regarding to attacks mentioned earlier, there are also a number of classic and state-of-the-art techniques proposed to fight against these problems (see section 2). Unfortunately, many techniques proposed so far, in many cases, provide obscure or hard to interpret pieces of information which are time-consuming and also needed experts or forensic practitioners to do the final judgment or decision.

To provide assistance in digital forensics investigation, in this paper, a general framework designed and aimed to improve quality of detection results against audio and image splicing forgery is introduced. Unlike traditional approaches, this framework was designed to combine results from any two different existing detection techniques into a better one with higher quality. The proposed framework was designed as a general method which can be efficiently applied to various kind of detection mechanisms.

The rest of this paper is organized as follows. Section 2 explains some background information about digital media forensics focusing on protection methods and attacks on digital image and audio. Section 3 introduced the main idea and details of our proposed framework following with experimental details and some sample results in section 4. In section 5, further analysis and discussion over developed framework are presented. Finally, we briefly conclude and point out our further research directions in section 6.

2. BACKGROUND AND RELATED WORKS

In this section, some background information about attacks and detection methods are classified and briefly conclude. The following subsections explain types of media forgery, today's detection techniques and also some similarity measuring methods respectively.

2.1 Types of Digital Media Forgery

In this paper, digital audio and image forgeries are divided into two major categories: *single-source* and *multiple-source forgery*. Regarding multiple-source forgery, this type of forgery is done by employing pieces of information from another source of media (e.g. digital image fragment from other digital images) and use them to perform manipulation (e.g. replace, merge, or insert) on the target media. Splicing is a forgery technique mainly belonged to this category.

Unlike multiple-source forgery, single-source media forgery involves only one source of media. The manipulation can be done by various approaches, e.g. deletion, duplication, insertion, etc. Example of forgery techniques belonged to this category are Copy-Move forgery (CMF) (Warif et al., 2016), image's properties adjustment (e.g. blurring, cloning, healing, brightness and contrast adjustment), audio deletion, etc.

2.2 Types of Forgery Detection Technique

Media forgery detection techniques can normally be classified into two categories: active and passive detection mechanisms. In the following subsection, the main concept of active and passive detection methods together with some classic and state-of-the-art detection techniques are briefly introduced.

2.2.1 Active Detection Methods

In this type of detection mechanism, additional pieces of information are inserted into the target digital media, i.e. photo or audio, at the time of its creation. Watermarking is a great example of this type of detection mechanism.

Watermarking (Wolfgang & Delp, 1997) is done by inserting pieces of identification information into the target media. The inserted data is spread across the entire media. Hence, during the investigation, forensic practitioners can verify the authenticity of the target digital media by observing consistencies of watermarking information within each section of the target media. Tampering of the target media can be efficiently determined by observing whether watermarking information in each section is corrupted/modified or not. Note that watermarking information is, generally, designed to be hard or impossible for attackers to remove, reverse or reconstruct.

2.2.2 Passive (Blind) Detection Methods

Unlike active detection, passive (so-called "blind") detection method requires no prior knowledge of the target suspected digital media. Passive detection method mainly relies on analyzing and finding inconsistencies of some information, properties or statistics lied within the target digital media. The inconsistencies of this information will lead to the finding of anomalies or tampered regions. The following are some reviews on interesting detection techniques for both image and audio forgery detection respectively.

Regarding the digital image, *blind noise estimation*, proposed by Mahdian, B. et al. (Mahdian & Saic, 2009) and Pan, X. et al. (Pan, Zhang, & Lyu, 2011), is one of the most common and widely discussed techniques in detecting image forgery. The method is achieved by estimating level/variance or distribution of noise on each part of the target image. Inconsistencies in these statistical values are used to determine an authenticity of the target digital photo; moreover, this information, in case of forgery, can also be used to locate the regions of tampering.

Concerning on JPEG compression characteristics, proposed by Farid, H. et al (Farid, 2009), a technique utilizing a property of JPEG digital image, so-called *"JPEG ghosts"*, is introduced. Generally, due to digitizing processes and quantization, a nature JPEG image will have the same level of information loss throughout the entire image. However, the tampered image, especially

spliced digital images, will have different levels of loss between tampered and non-tampered areas. These inconsistencies in levels of loss are important clues leading to the finding of anomalies within target digital photos.

Another interesting technique in detecting digital image forgery is using of *image interpolation information*. Normally, altering a digital image, in many cases, involves two processes: transformation and re-sampling. By performing these processes, an interpolation process is invoked. Hence, it is possible to use the characteristic and patterns lied within interpolated digital images in detecting image forgery.

There is a number of research and study involving interpolation characteristics of a digital image (Takamatsu, Matsushita, Ogasawara, & Ikeuchi, 2010). By applying a statistical function on the digital enlarged image, a method of detecting a type of interpolation being used in target JPEG compressed digital images (i.e. linear and cubic interpolation) was proposed.

In 2013, Hwang and Har (2013) had proposed a novel approach in detecting image forgery by using re-interpolation algorithm. By applying *Discrete Fourier Transform (DFT)* (Roberts, 2003) on target digital image, the obtained characteristics are used to indicate a rate of interpolation. Regarding DFT conversion results, the digital image with higher interpolation rate will lead to the lesser amount of high-frequency elements. Using DFT and image scaling, the detection results (so-called "detection map") is created in order to locate the tampered areas.

Regarding digital audio, there are also several passive detection techniques designed in order to detect audio forgery proposed and discussed in the literature. For example, an audio forgery detection method using pitch similarity is introduced in (Yan, Yang, & Huang, 2015).

Similar to the digital image, *noise estimation technique* can also be applied to digital audio in order to determine the authenticity of the target suspected audio signal. The main idea of this method is to measure and observe the level/variance of noise in each audio sections of the given audio signal. Inconsistencies of noise level between each audio section will lead to finding and locating of tampered regions within the suspect digital audio. A good example of using local noise estimation technique in detecting audio forgery was introduced by Pan, Zhang, and Lyu (2012).

In 2011, using *Singular Value Decomposition (SVD)* (Kannan & Hopcroft, 2012) as core mechanism, a detection technique for digital audio was proposed by Shi and Ma (2011). In this technique, SVD is employed in order to express linear dependencies of values within the given digital audio signal. The detection is achieved by first performing SVD on the target audio signal. Counting and calculating the average of the number of zero singular values within the obtained SVD results, the calculated results can be used in describing and indicating statistical changes leading to the finding of anomalies lied within the target digital audio signal.

2.3 Similarity Measuring Methods

Regarding methods for measuring similarity level between two sets of data, there is a number of techniques and studies previously proposed and discussed in the literature. In the following subsections, details of some interesting similarity measuring mechanisms are briefly described.

2.4 Pearson's Correlation

Pearson's correlation (Andale, 2012) is a statistical technique designed to measure the level of linear dependency within the given set of data. The measurements result in a single value between $[-1, +1]$. where $+1$, -1 and 0 indicate total positive, total negative and no correlation respectively. Figure 2 shows an example of Pearson's correlation approach.

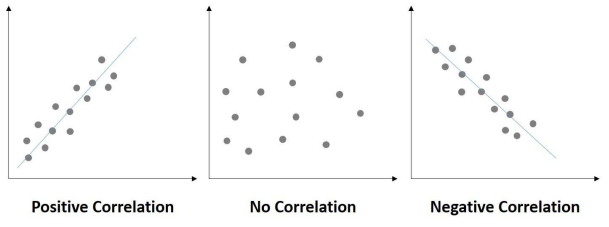

Figure 2: General concept of Pearson's correlation method.

2.5 2-D Cross Product

Unlike Pearson's correlation or other similarity measuring technique, in this paper, we also introduce a new way of measuring similarity or dependency between two sets of data using 2-D cross product.

Let us assume that we have two sets of data A and B. This method is achieved by first computing the principal vector $\vec{P}$ using variance, average or any property that spread through both entire set of data A and B.

$$\vec{P} = \begin{bmatrix} var(A) \\ var(B) \end{bmatrix} \tag{1}$$

The vector $\vec{P}$ is a reference vector which now acts as representative of both A and B. We, then, equally divide A and B into fixed-size data blocks and for each corresponding block from A and B, we create a regional vector $\vec{V}(i)$, where i indicates the target block's number.

$$\vec{V}(i) = \begin{bmatrix} var(A(i)) \\ var(B(i)) \end{bmatrix} \tag{2}$$

By perform cross product between $\vec{P}$ and each regional vector $\vec{V}(i)$, the results of each cross product performed give information about how much is the vector from that particular region $\vec{V}(i)$ different from the entire set of data $\vec{P}$. The results from these processes can be used to indicate the level of dependency or separate two set of data from each other; this method, however, may not has high accuracy when comparing to another method including Pearson's correlation.

3. PROPOSED FRAMEWORK

In this section, a new framework designed to improve the efficiency of today's digital media (i.e. image and audio) forgery detection is introduced. The enhancement begins with performing of two traditional forgery detection techniques on the target digital media. The detection results obtained by each method, then, are combined using combination or similarity measuring techniques, e.g. cross-product, Pearson's correlation, etc. Details of our proposed framework are presented as follows.

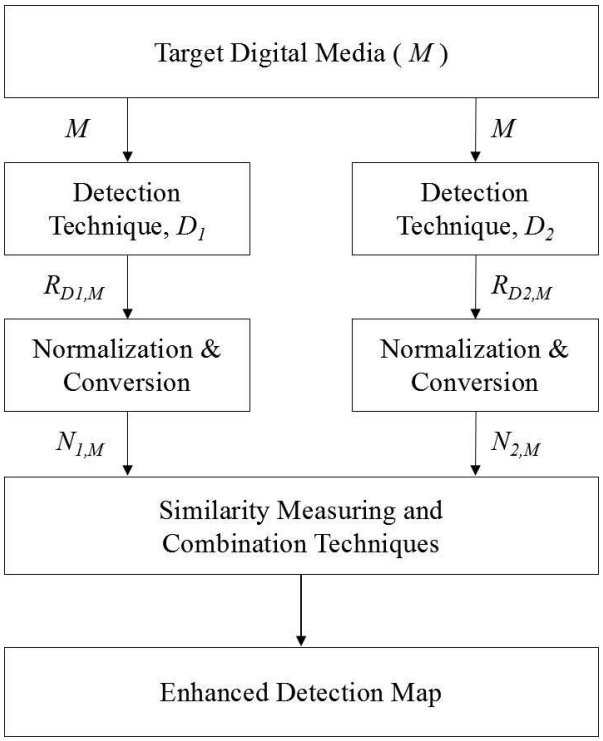

Figure 3: Overview of our proposed mechanism.

Figure 3 presents an overview of our proposed framework. Let us assume that we are trying to enhance forgery detection results by using the combination of two existing detection techniques: D_1 and D_2 on the target digital media M.

The enhancement procedures involving the following steps. First, we perform detection technique D_1 and D_2 on target digital media M resulting in $R_{D1,M}$ and $R_{D2,M}$ respectively.

Next, the obtained detection results from the previous step are normalized; moreover, domain conversion will also be applied in the case that two detection results do not belong to the same domain, e.g. time and frequency domain. Conversion is normally done by using *Fast Fourier Transform (FFT)* (Bergland, 1969).

Following to normalization and conversion processes, the similarity measuring techniques (e.g. cross/inner product, Pearson's Correlation, Cross-correlation, etc.) are employed in order to measure the similarity between these two data segments. The results from similarity compari-

son are used to generate a new set of data called *"Enhanced Detection Map"*. This enhanced detection map is served as a newly improved version of detection results in which tampered areas are more clearly highlighted comparing to results from traditional methods D_1 and D_2.

According to the concept and idea described, the implementation processes involve four following steps:

Step 1: As shown in figure 3, let us assume that we trying to combine detection results of a target digital image M, derived from two digital image forgery detection techniques D_1 and D_2, into an enhanced detection result with higher quality and easier to be interpreted. First, we perform digital image forgery detection using traditional detection techniques D_1 and D_2:

$$R_{D1,M} = D_1(M) \tag{3}$$

$$R_{D2,M} = D_2(M) \tag{4}$$

where $D_1(M)$ and $D_2(M)$ represent performing of forgery detection using technique D_1 and D_2 over the target digital media M. The results are denoted as $R_{D1,M}$ and $R_{D2,M}$ respectively.

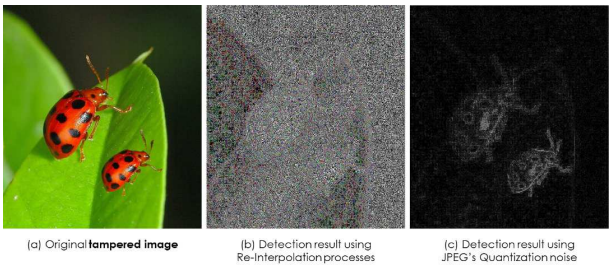

Figure 4: An example of digital image tampering detection using re-interpolation processes and JPEG's quantization noise.
Source: *CASIA Tampered Image Detection Evaluation Database* (2009)

Let us assume that $R_{D1,M}$ and $R_{D2,M}$ represent JPEG's quantization noise (Farid, 2009) and re-interpolation based techniques (Hwang & Har, 2013) respectively. Figure 4 show an example of digital image tampering detection using today's traditional mechanisms.

Step 2: By obtaining detection results from both D_1 and D_2, we then normalize value of all elements inside $R_{D1,M}$ and $R_{D2,M}$. By scaling these values, the value of each element in the normalized results $N_{1,M}$ and $N_{2,M}$ will share same range of value (0 to 1, for example).

In some cases, results from $R_{D1,M}$ and $R_{D2,M}$ may not belong to the same domain, e.g. time and frequency domains. Hence, some transformation processes (Fast Fourier Transform, for instance) are needed to perform prior to normalization processes.

Step 3: Upon retrieving normalized detection results $N_{1,M}$ and $N_{2,M}$, we then divide $N_{1,M}$ and $N_{2,M}$ into n fixed-size data fragments. Results of this processes are denoted as $N_{1,M}(i)$ and $N_{2,M}(i)$, where $1 \leq i \leq n$.

Step 4: In this step, we then perform the combination of detection results by using similarity measuring mechanism; e.g. 2-D cross product, Pearson correlation, etc.

Let us assume that we are combining detection results of the target digital image by using 2-D cross product (see section 2.3 for more information) as a core mechanism. We first create regional vectors $\vec{V}(i)$, a set of vectors representing each pair of data fragments $(N_{1,M}(i), N_{2,M}(i))$, where $1 \leq i \leq n$ as follows:

$$\vec{V}(i) = \begin{bmatrix} var(N_{1,M}(i)) \\ var(N_{2,M}(i)) \end{bmatrix} \tag{5}$$

Next, we create a principal vector $\vec{P}$ as a reference vector representing two entire detection results.

$$\vec{P} = \begin{bmatrix} var(N_{1,M}) \\ var(N_{2,M}) \end{bmatrix} \tag{6}$$

With principal and regional vectors, we, finally, perform similarity measurement by computing cross product between $\vec{P}$ and each element in $\vec{V}(i)$. The enhanced version of detection result is denoted as $M(i)$ where $1 \leq i \leq n$.

$$\vec{M}(i) = \vec{P} \times \vec{V}(i) \tag{7}$$

Step 6: As final results, the practitioner can consequently plot $M(i)$ in order to view and analyze the enhanced detection results. The following figure shows the comparison between our

enhanced detection results and the traditional ones.

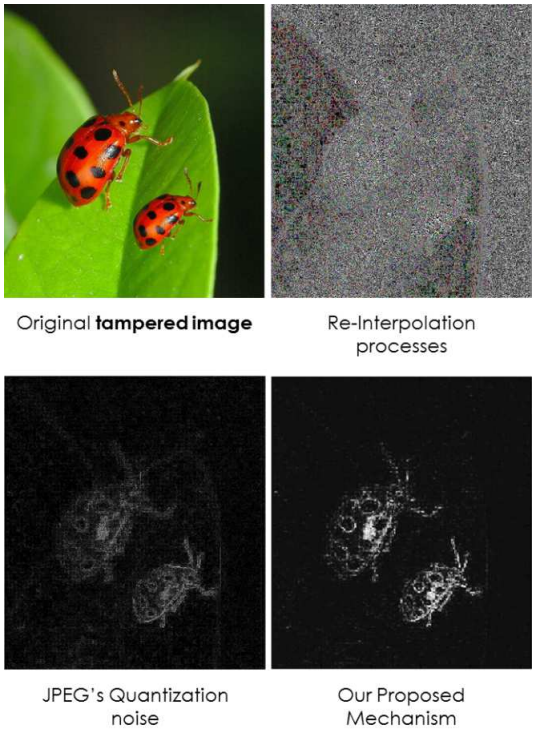

Figure 5: Comparison between enhanced and traditional forgery detection results.
Source: *CASIA Tampered Image Detection Evaluation Database* (2009)

As we will see, in figure 5, the proposed mechanism can efficiently improve the quality of the detection results. With this improvement, the proposed framework not only can aid experts/forensic practitioners but also help non-experts or non-skilled personnel in their basic forensic investigation.

Furthermore, regarding digital audio, this framework can also achieve the same goal by changing the target media from digital image to an audio signal and then the user may replace the similarity measuring technique (i.e. 2-D cross-product) to another technique, e.g. Pearson's correlation.

4. EXPERIMENT RESULTS

The experiment was conducted utilizing MATLAB version 9.1.0.441655 (R2016b). Regarding the digital image, *CASIA Tampered Image Detection Evaluation Database* (2009), a public dataset of color digital images consisting of 7,491 authentic and 5,123 tampered digital images, was adopted during the test. Concerning audio signal used in the experiment, we create our own realistic forged audio signal in order to test the efficiency of our proposed mechanism. The following subsections show experiment results on digital image and audio respectively.

4.1 Results on Digital Images

In our experiment on digital images, three traditional detection methods were used in performing combinations; JPEG's quantization noise, re-interpolation, and noise estimation approach.

Figure 6 shows our enhanced detection results compared to traditional approaches.

As we will see, in figure 6, first, the re-interpolation technique usually show some inconsistencies in pattern between authentic and tampered regions. The quality of results from re-interpolation processes is, unfortunately, poor making it extremely hard for the practitioner to interpret or precisely locate forged region lying within the target tampered digital image.

Second, concerning the using of JPEG's quantization noise, this technique can efficiently locate forged regions of the target digital image. However, this technique also usually give us some irrelevant noise which may obscure or hinder the investigation processes. Moreover, JPEG's quantization technique is also weak against low-quality JPEG tampered image.

Finally, regarding noise estimation, this technique generally give information about the level of noise in each section of the target digital image. With noise information, the forensic practitioner can verify the authenticity of a target image by looking for inconsistencies of the noise level in each area. This technique is simple and easy to implement; however, this technique works well only when the tampered and non-tampered area within the target image have significant differences in noise levels. In many cases where noise level of tampered and non-tampered regions have values close to each other, the quality of the detection result will drop drastically.

As we will see, each technique used in com-

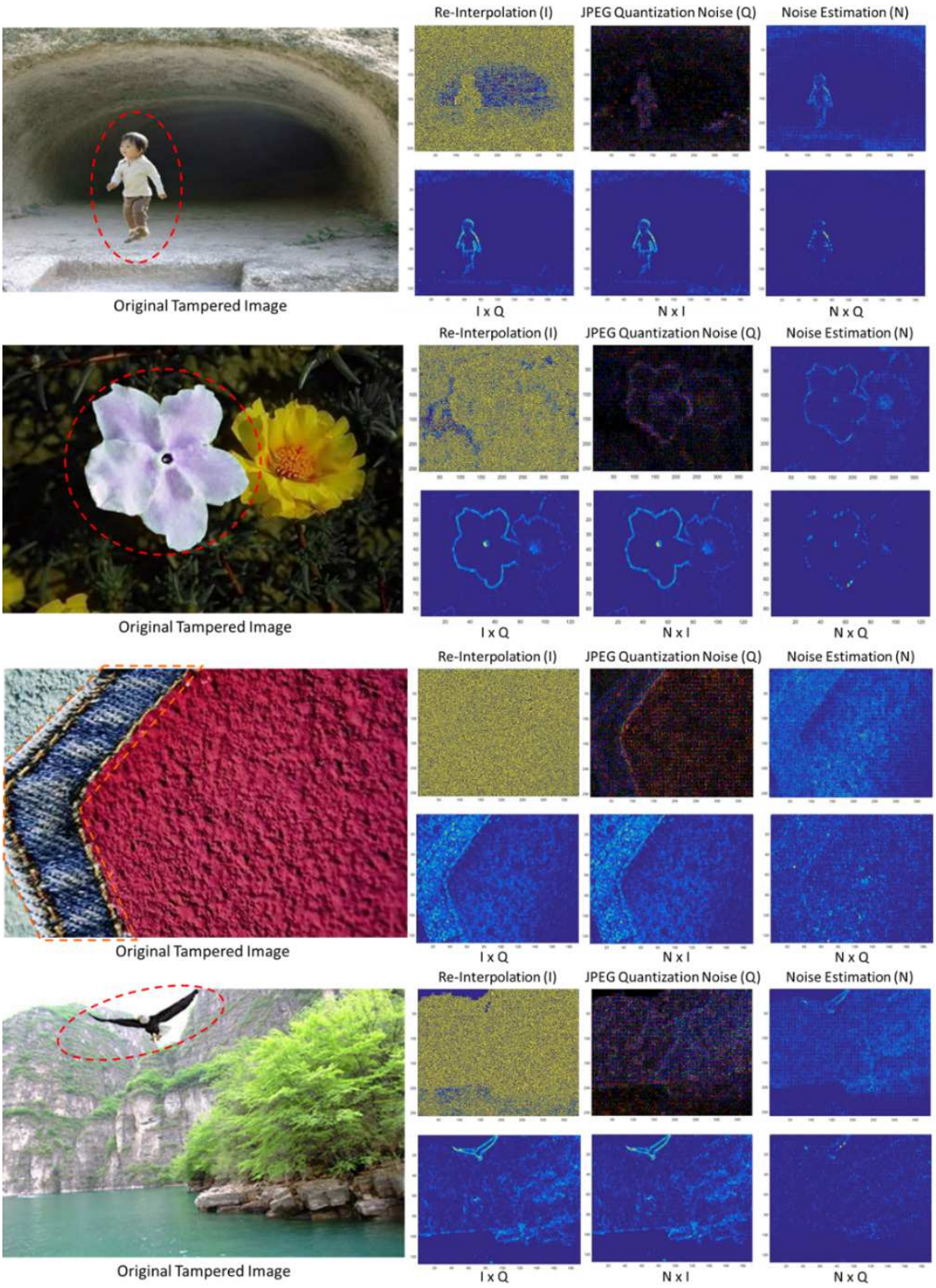

Figure 6: Experiment results on tampered digital images
Source: *CASIA Tampered Image Detection Evaluation Database* (2009)

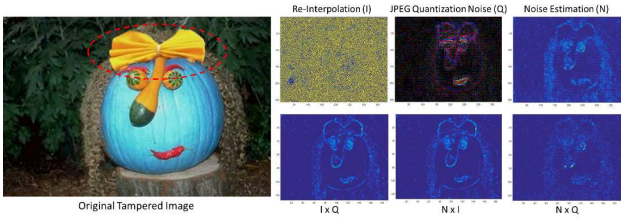

Figure 7: An unsuccessful example of our developed method

Source: *CASIA Tampered Image Detection Evaluation Database* (2009)

bination have their own benefits and drawbacks. With our developed combining mechanism, the quality of detection results is now improved leading to easier and more accurate interpretation and forensic investigation. Our developed framework, however, is not a silver bullet solution. There are also chances of producing false negative or poor quality results as well. Figure 7 shows an unsuccessful example of our developed mechanism.

According to this example, the JPEG's quantization and noise estimation technique show both false positive, i.e. the algorithm has indicated that some parts of the target image were tampered which are actually not. Considering re-interpolation method, the obtained detection result is very noisy; anomalies are appeared on both yellow ribbon and the rest of the target image. With this result, it is hard to accurately determine authenticity and locate the tampered area (i.e. yellow ribbon) on the target image.

Using these defective detection results in combination, the error from each detection result from both techniques will be magnified. As a result, the final detection result using our developed mechanism will also show the defective (false positive) result which will not be useful for forensic investigators and may also hinder non-skilled personnel during their investigation.

4.2 Results on Digital Audio

In this experiment, noise estimation (Pan et al., 2012) and SVD-based technique proposed by Shi and Ma (2011) were used in performing combination. Moreover, Pearson's correlation was also adopted as core similarity measuring function.

Figure 8 shows experiment results of our developed framework comparing with results from traditional approaches.

Figure 8 shows the comparison between our developed framework and two traditional approaches, i.e. SVD-based and noise estimation method. The first and third rows, target audio signals are spliced using two different sources of audio while the second sample (one in the middle) are forged using three different audio sources.

In this experiment on digital audio, we have found that increasing of audio sources used in forging a spliced audio will also increase the difficulty in detecting anomalies within that particular audio file. This also affects our proposed framework. Regarding the second sample created using three different sources of audio, this audio signal, in this case, contains two points of tampering/anomalies. The enhanced results, however, explicitly shows only the first point of tampering while the clarity of the second anomaly was significantly lowered (i.e. lesser amplitude and looking rather obscure). Figure 9 explains the problem mentioned earlier in detail.

5. DISCUSSION AND ANALYSIS

In this paper, we present a general framework for enhancing the quality of detection results obtained from today's forgery detection techniques. The proposed framework was designed as a general framework in which can be applied with any passive(blind) detection techniques.

Utilizing our developed framework, the quality of detection results are significantly increased. With this improvement, it can support not only skilled-personnel (e.g. forensic practitioners) but also non-skilled personnel during their digital forensics investigation.

The proposed mechanism works well in detecting spliced media and also locating anomalies within the target tampered media (i.e digital image or audio). The proposed method, however, is still weak against single-source manipulation, e.g. deletion and copy-move forgery (CMF).

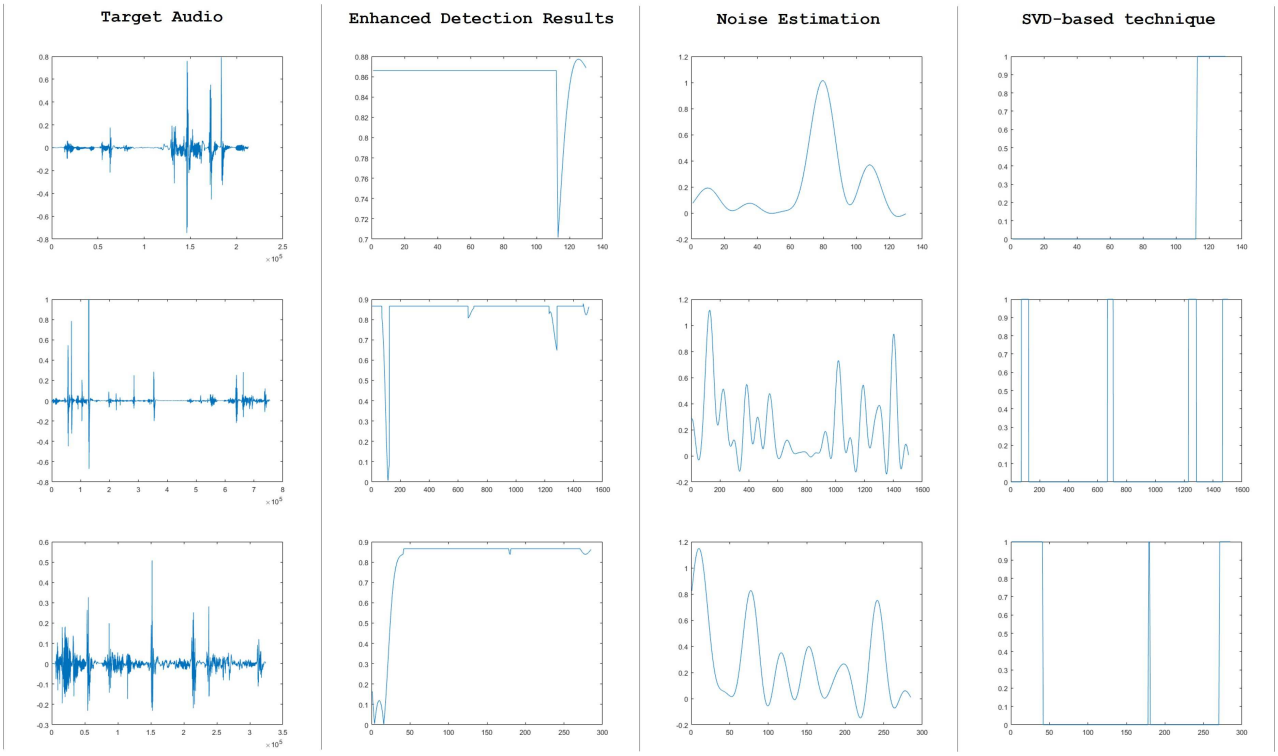

Figure 8: Experiment results on tampered digital audio

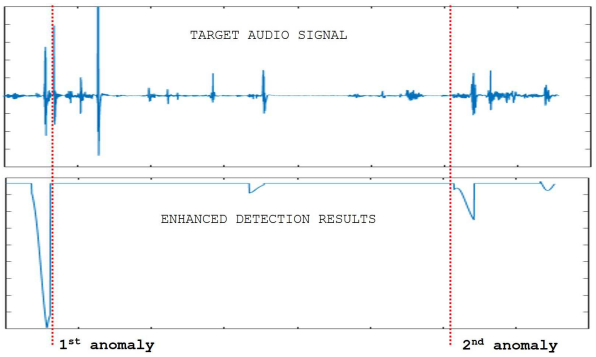

Figure 9: Effect of increasing audio sources in a spliced audio.

Concerning the number of media sources used in forging target spliced media, the increasing number of media sources has a significant negative impact on the quality of the enhanced results. The larger number of media sources are used in forging the lesser quality the enhanced detection results have become.

Regarding the use of similarity measuring technique as the crux of the combination mechanism, in this paper, we introduce the use of Pearson's correlation and 2-D cross product. These two methods, however, can also be replaced with other similarity measuring function (cross-correlation (Bourke, 1996), inner product, for example) which might yield better results.

Finally, about the implementation, the results from traditional techniques used in combination are divided into fixed-size windows in which a predetermined window-sized is necessary. Moreover, in some detection techniques, threshold/predefined values are required, Shi and Ma (2011), for instance. Selecting the optimum value for these predetermined values (especially window-size), therefore, still requires more studies and observations which is also left as an open challenge for future research.

6. CONCLUSION

We present a new general framework for enhancing today's digital image and audio forgery detection. The proposed method was designed as a general tool which can be applied with

any passive/blind media forgery detection techniques. The enhanced version of detection results clearly shows tampered regions within the target suspected media. With this improvement, this framework can help providing support for both experienced forensic practitioner and non-skilled personnel during their forensic investigation. The proposed method, however, also has its own drawback regarding the dropping of detection result's quality upon increasing of media sources used in splicing the target media and the use of predetermined/threshold values which are left as open challenges for further studies.

REFERENCES

A. Muller, R. (2004). *The Voice of Osama bin Laden.* Retrieved 2016-10-22, from https://www.technologyreview.com/s/402415/the-voice-of-osama-bin-laden

Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Science International*, *231*(1-3), 284–295. Retrieved from http://dx.doi.org/10.1016/j.forsciint.2013.05.027 doi: 10.1016/j.forsciint.2013.05.027

Andale. (2012). *Pearson Correlation: Definition and Easy Steps for Use.* Retrieved 2016-02-17, from http://www.statisticshowto.com/what-is-the-pearson-correlation-coefficient/

Bergland, G. (1969). A guided tour of the fast Fourier transform. *Spectrum, IEEE*, *6*(7), 41–52. Retrieved from http://ieeexplore.ieee.org/xpls/abs{_}all.jsp?arnumber=5213896 doi: 10.1109/MSPEC.1969.5213896

Birajdar, G. K., & Mankar, V. H. (2013, oct). Digital image forgery detection using passive techniques: A survey. *Digital Investigation*, *10*(3), 226–245. Retrieved from http://www.sciencedirect.com/science/article/pii/S1742287613000364 doi: 10.1016/j.diin.2013.04.007

Bourke, P. (1996). *Cross Correlation.* Retrieved from http://paulbourke.net/miscellaneous/correlate/

CASIA Tampered Image Detection Evaluation Database. (2009). Retrieved from http://forensics.idealtest.org/casiav2/

Chakraborty, A., Paranjape, B., Kakarla, S., & Ganguly, N. (2016). Stop Clickbait: Detecting and preventing clickbaits in online news media. In *Proceedings of the 2016 ieee/acm international conference on advances in social networks analysis and mining, asonam 2016* (pp. 9–16). doi: 10.1109/ASONAM.2016.7752207

Farid, H. (2009). Exposing digital forgeries from JPEG ghosts. *IEEE Transactions on Information Forensics and Security*, *4*(1), 154–160. doi: 10.1109/TIFS.2008.2012215

Hwang, M. G., & Har, D. H. (2013). A Novel Forged Image Detection Method Using the Characteristics of Interpolation. *Journal of Forensic Sciences*, *58*(1), 151–162. doi: 10.1111/j.1556-4029.2012.02265.x

Kannan, R., & Hopcroft, J. (2012). *Computer Science Theory for the Information Age.*

Lappin, Y. (2006). *Reuters admits altering Beirut photo.* Retrieved 2016-09-06, from http://www.ynetnews.com/articles/0,7340,L-3286966,00.html

Mahdian, B., & Saic, S. (2009, sep). Using noise inconsistencies for blind image forensics. *Image and Vision Computing*, *27*(10), 1497–1503. Retrieved from http://www.sciencedirect.com/science/article/pii/S0262885609000146 doi: 10.1016/j.imavis.2009.02.001

Nizza, M., & J. Lyons, P. (2008). *In an Iranian Image , a Missile Too Many.* Retrieved 2017-07-10, from http://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many

Pan, X., Zhang, X., & Lyu, S. (2011). Exposing image forgery with blind noise estimation. In *Proceedings of the thirteenth acm multimedia workshop on multimedia and security - mm&sec '11* (p. 15).

Retrieved from http://dl.acm.org/citation.cfm?doid=2037252.2037256 doi: 10.1145/2037252.2037256

Pan, X., Zhang, X., & Lyu, S. (2012). Detecting Splicing in Digital Audios using Local Noise Level Estimation. In *Proceedings of the 2012 ieee international conference on acoustics, speech and signal (icassp)* (pp. 1841–1844). doi: 10.1109/ICASSP.2012.6288260

Roberts, S. (2003). *Lecture 7 - The Discrete Fourier Transform.* Retrieved from http://www.robots.ox.ac.uk/{~}sjrob/Teaching/SP/l7.pdf doi: 10.1142/4610

Shi, Q., & Ma, X. (2011). Detection of audio interpolation based on singular value decomposition. *2011 3rd International Conference on Awareness Science and Technology (iCAST)*, 287–290.

Sundaram.A, M., & Nandini, C. (2015). Image Retouching and it's Detection - A Survey. *International Journal of Research in Engineering and Technology*, *04*(14), 30–34.

Takamatsu, J., Matsushita, Y., Ogasawara, T., & Ikeuchi, K. (2010). Estimating demosaicing algorithms using image noise variance. In *Proceedings of the ieee computer society conference on computer vision and pattern recognition* (pp. 279–286). doi: 10.1109/CVPR.2010.5540200

Warif, N. B. A., Wahab, A. W. A., Idris, M. Y. I., Ramli, R., Salleh, R., Shamshirband, S., & Choo, K. K. R. (2016). Copy-move forgery detection: Survey, challenges and future directions. *Journal of Network and Computer Applications*, *75*, 259–278. Retrieved from http://dx.doi.org/10.1016/j.jnca.2016.09.008 doi: 10.1016/j.jnca.2016.09.008

Wolfgang, R. B., & Delp, E. J. (1997). a Watermarking Technique for Digital Imagery : Further Studies. In *Proceedings of the international conference on imaging, systems, and technology* (pp. 279–287). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.18.8994

Yan, Q., Yang, R., & Huang, J. (2015). Copy-move detection of audio recording with pitch similarity. *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, *2015-August*(61202497), 1782–1786. doi: 10.1109/ICASSP.2015.7178277