Computers and Electrical Engineering 63 (2017) 41–52

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

# Enhancement of multimedia security using random permutation with wavelet function☆

M.S. Gouri*, R.V. Siva Balan

*Department of Computer Science and Engineering, Noorul Islam University, Kanyakumari District, Tamilnadu, India*

ARTICLE INFO

*Article history:*
Received 14 March 2017
Revised 9 September 2017
Accepted 11 September 2017

*Keywords:*
Digital multimedia
Pseudo arbitrary permutation
Haar wavelet coefficients
Translation-invariance wavelet transform

ABSTRACT

Digital data include financial documents and medical records, where security is not guaranteed. Unfortunately, cybercrime has developed for several multimedia applications. To overcome cybercrime, forensic analysis is applied. However, an increasing amount of malware is embedded in video payloads, and to minimize this amount, pseudo arbitrary permutation of movable Haar wavelet coefficients (PAP-MHWC) was developed. Pseudo arbitrary permutation using a secret key is permutated to decrease the probability of malware and reduce the distortion rate. Forensic security collects log file information as verification. Haar wavelet coefficients are a sequence of square-shaped functions used in a Fourier analysis to identify cyber forensic regions in video files. Such coefficients enable working with increasingly complex files by decomposing them into various positions and scales. Video frame overlapping is removed using a translation-invariance wavelet transform, thereby improving the forensic security rate. Experiment results show that the proposed PAP-MHWC method achieves a better performance in terms of malware detection accuracy, false-positive ratio, malware detection time, and malware crime probability rate than previous methods.



## 1. Introduction

Cyber forensics is the course of collecting information and data from computers used as digital proof for civil purposes, and to confirm and officially act against cybercrime. Cyber forensics also includes the act of constructing digital data suitable for application to a criminal investigation. Digital and multimedia sciences are a rising field in forensic sciences. In addition, forensic computer investigators, i.e. digital scientists, locate, identify, and preserve digital evidence such as those found on computer hard drives, email systems, cameras, CDs, and other types of media.

The digital forensic process is a predictable scientific and forensic method used in a digital forensic analysis. There are four types of processes involved in a digital forensic investigation: evidence collection, examination, analysis, and reporting.

The four phases of a digital forensic investigation are listed in Fig. 1. In the first phase, the label, record, and digital data or videos are recognized from the possible sources. An examination is the task of handling a large amount of collected data using different computerized and manual methods to evaluate and extract relevant data.

The next phase of the process is to analyse the results of the examination with acceptable authorization methods and techniques and to obtain useful information that addresses the questions posed by the group performing the collection and

☆ Reviews processed and recommended for publication to the editor-in-chief by associate editor Dr. R. Varatharajan.

* Corresponding author.
*E-mail addresses:* msgouriphd@gmail.com, gourimohans@gmail.com (M.S. Gouri), rvsivan@gmail.com (R.V.S. Balan).

http://dx.doi.org/10.1016/j.compeleceng.2017.09.014
0045-7906/

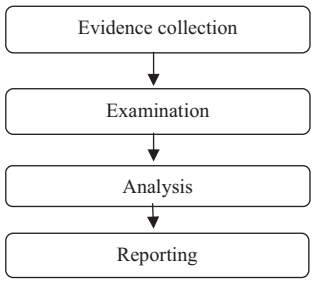


**Fig. 1.** Stages of digital forensic process.

examination. The final phase is reporting the results of the analysis, which consists of relating the procedures used, describing the tools and events that were chosen, finding other actions that need to be carried out, and providing implications for improvement plans, procedures, measurements, tools, and other features of the forensic process. Based on the process model, our proposed methods were built to remove malware from digital videos using Haar wavelet coefficients and pseudo arbitrary permutation.

A sparse-reconstruction based metric-learning method [1] used the point-to-set distance metric. However, this type of system has not been applied to other computer vision applications such as face and object cyber forensic recognition in video files. In a preliminary forensic analysis of an Xbox One [2], the video game log file was saved on a hard drive. The hard drive contains the timestamps of the gaming discussion, including the time, date, and span. The added security features caused significant complexity in forensically acquiring digital forensic artefacts. In [3], a forensic analysis of video file formats employed different container formats and compression codecs for transfer from the sender to the receiver end. However, security specifications regarding the lossless video editing and compression of the original video stream for video files were not automated.

A curriculum package for digital forensics was developed in [4] to deal with the large quality digital forensic education curriculum. Some security concerns associated with digital archiving systems were presented in [5], which also provides various security requirements for a digital archive scheme. However, the paper did not focus much on security issues or the requirements for securing digital archives. A novel technique was developed in [6] to identify and track video text in any direction using spatial and temporal information. However, this technique did not address the security of a video text.

A sequence-alignment method was introduced in [7] for identifying complex data-leak patterns and long and incorrect sensitive data patterns. However, this method failed to detect data-movement tracking. Binary image steganographic methods for reducing distortion in a texture were introduced in [8], which can also be used to improve the statistical security without changing the image quality.

A high payload watermarking method was described in [9] for high-efficiency video coding. The efficiency of the video compression standard increased, providing a better compression performance. However, the robustness of the method was not developed. In [10], a two-stage semantic model-building method was introduced into the video concept indexing model for dealing with semantic information. Therefore, the challenge lies in a security enhancement of the digital video framework that overcomes the limitations of existing works.

In this paper, an efficient pseudo arbitrary permutation of movable Haar wavelet coefficients (PAP-MHWC) method is introduced to reduce malware in multimedia content such as digital videos. Haar wavelet coefficients are a sequence of square-shaped functions applied with a Fourier analysis to identify a cyber forensic region of a video file. Haar functions also operate with an increasing size of the embedded video payload to identify a malware incident. To enhance the forensic security of a multimedia video, a pseudo arbitrary permutation with a secret key, $S$, is applied. Pseudo arbitrary permutation minimizes the malware crime probability rate. Haar wavelet coefficients of the video enable working on complex video frames by decomposing them into different positions and scales. A translation-invariance wavelet transform (TIWT) is used to increase the forensic security rate.

The rest of this paper is organized as follows: Section 2 discusses cyber forensic security providence for multimedia digital data, Section 3 provides a description of the proposed PAP-MHWC method applied to multimedia digital video, Section 4 presents a performance evaluation, Section 5 describes the experimental settings, Section 6 discusses the results, and finally, Section 7 provides some concluding remarks.

## 2. Related work

Cybercrime applied to digital data occurs through the communication channel. A cryptographic technique was introduced in [11] for authenticating and securing medical images in health information systems. However, the image pixel values are distorted during the watermarking process.

An efficient multimedia encryption method [12] was used for real-time video data in an embedded video sensing method. A security method based on watermarking and encryption was developed in [13] for digital imaging and communications in medicine. It offers patient authentication, information privacy, and reliability based on the watermark.