Novel Forensic And Anti-Forensic Techniques Identification Based On Game Theory Frame Work

Geetha S Raveendran
PSN College of Engineering and Technology
Tirunelveli, Tamilnadu

R. LakshmiPriya
PSN College of Engineering and Technology
Tirunelveli, Tamilnadu

Abstract

Digital crimes are increasing day by day. So digital forensic is an imperative technique for collecting evidences. Computer forensics involves the conservation, recognition, mining, elucidation, and documentation of computer evidence. Digital forensics uses digital data as an evidence for investigating a crime. Similarly, several anti-forensic operations have recently been designed to make digital forgeries barely discernible by forensic techniques. Anti-forensic techniques are designed to give the wrong impression about forensic analysis by erasing or falsifying palm vein videos left by editing operations. In this paper we are introducing palm vein authentication instead of finger prints that use blood vessel pattern as a personal identifying factor for detecting forgery. Duplication of vein information is very difficult, because the veins are internal to the human body. In palm vein authentication considering vascular patterns of an individual's palm as personal identification. The palm vein authentication technology offers a high level of precision compared with a fingerprint analysis. A palm has a broader and more difficult vascular pattern, so it is difficult to differentiate features for personal identification.

Keywords *- Game theory, image compression, forensic techniques, anti-forensics techniques, Palm vein authentication.*

1. Introduction

In recent years, forensic and anti-forensic techniques have become increasingly ubiquitous throughout the police department for digital video/image manipulation. Digital forensic techniques seek to provide information about digital multimedia content without relying on external descriptors such as metadata tags or extrinsically entrenched information such as digital watermarks. Forensic techniques have been developed to perform a variety of tasks such as detecting evidence of editing or forgery, identifying media file's origin, and tracing multimedia content's processing history for digital images [2], [3], [10], [12] video [11], [13], [14].Digital forensic techniques have become extremely important to verify the integrity of digital content, because multimedia content can be easily altered using digital editing software. In former work, anti-forensic techniques are designed to give the wrong impression about forensic analysis by erasing or falsifying fingerprints left by editing operations. Anti-forensic techniques have been anticipated to remove traces of image resizing and rotation and forge the photo-response non-uniformity (PRNU) Palm vein blood vascular patterns image by a digital camera's electronic sensor.

Anti-forensic techniques have been proposed to erase or falsify an image's compression history [1], [7], [8].These techniques can be used to bamboozle forensic algorithms that recognize image forgeries by searching for inconsistencies in an image's compression history [6], [12]. Anti-forensic techniques designed to remove forensically significant indicators of compression from an image [1]. Anti-forensic techniques also used for removing image's contrast enhancement and color filter array artifacts used for camera identification or fake detection. Digital editing operations leave behind blood vessel pattern, anti-forensic operations may inadvertently leave behind their blood vessel pattern [9].

Some anti-forensic technique capable of removing the temporal palm vein blood vascular patterns from videos that have undergone frame addition or deletion [4]. A number of techniques are available to evaluate the performance of anti-forensic algorithms along with a game theoretic framework for analyzing the interplay between forensics and anti-forensics. Furthermore, a new automatic video frame deletion detection technique along with a technique to detect the use of video anti-forensics [5]. If this blood vessel pattern can be identified, forensic techniques can be designed to detect them. This will allow forensic investigators to identify digital forgeries even when editing blood vessel pattern have been anti-forensically removed. Researchers have recently developed techniques to identify anti-forensic

manipulation of an image's PRNU [9] and compression history [15].

Biometrics refers to technologies used to detect and recognize human physical characteristics. The pattern of blood veins is unique to every individual, even among identical twins. Palms have a broad and complicated vascular pattern and thus contain a wealth of differentiating features for personal identification. Furthermore, it will not vary during the person's lifetime. It is a very secure method of authentication because this blood vein pattern lies under the skin. This makes it almost impossible for others to read or copy [16]. Difficult to forge because of palm veins are inside the superficial skin. It is impossible to copy the palm veins. It is highly accurate and capable of 1:1 and 1: many matching [17].

In this paper we are introducing palm vein authentication instead of finger prints. Duplication of vein information is very difficult, because the veins are internal skin. In palm vein authentication considering vascular patterns of an individual's palm as personal identification. The palm vein authentication technology provides high level of accuracy. The main contributions of this work can be summarized as follows:

- Palm vein authentication
- Palm vein segmentation
- Video P-frame prediction
- Frame Deletion or Addition
- Forensics and Anti-Forensics Techniques
- Game Theoretical frame work
- Detecting video forgery

Digital formatted video makes sense to compress for further usage. This compression mechanism is similar to normal image/video compression. We compress data for getting maximum quality and minimum storage space. This is correlated to both space and time domains. Most videos are coded with the JPEG standard. Therefore, the JPEG compression provides valuable clues that can be leveraged by the forensic analyst. In video coding, a group of pictures, or GOP structure, specifies the order in which intra and inter frames are arranged. The GOP is a group of successive pictures within a coded video stream. Each coded video stream consists of successive GOPs and from these pictures only visible frames are generated.

A GOP can contain the following picture types:

- I-frame (intra coded picture)
- P-frame (predictive coded picture)
- B-frame (bidirectional predictive coded picture).
- D-frame (DC direct coded picture)

A GOP always begins with I-frame and then several P-frames. Some frames distances are from each frame. In the remaining gaps are B-frames. Some video codices only allows for more than one I-frame in a GOP.

2. System architecture

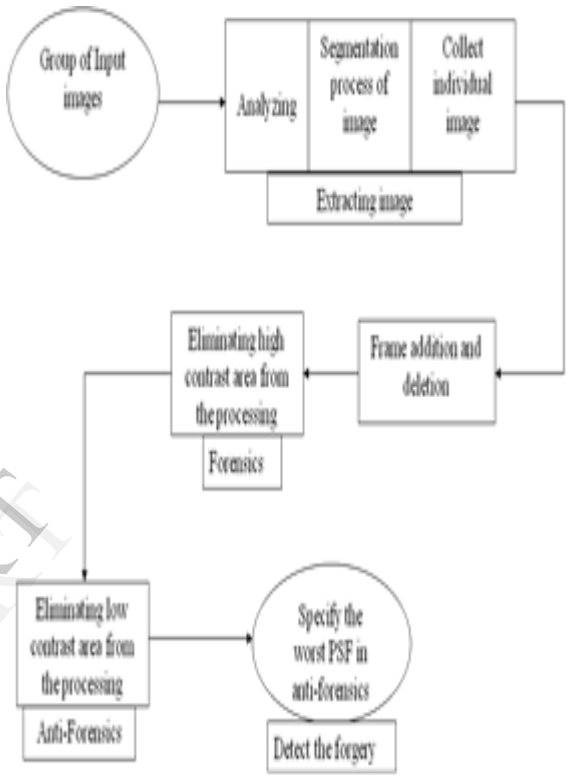

Figure.1. System architecture

3. Palm vein biometrics

Palms have a broad and complicated vascular pattern and thus contain a wealth of differentiating features for personal identification. It will not vary during the person's lifetime. Difficult to forge because of palm veins are inside the superficial skin. It is impossible to copy the palm veins. It is highly accurate and capable of 1:1 and 1: many matching. There are only seven companies in the world, who manufactures Palm Vein Recognition equipment and Mantra Softech India is one of them.

Applications of palm vein biometrics are

- Security systems: physical security
- Log-in control: Both network and PC access.
- Banking (ATM) and financial services
- Healthcare

3.1 Working of Palm Vein Biometrics

An individual's or group of peoples vein pattern video is captured by radiating his/her hand with near-infrared rays. Some far infrared ray based vein image capturing techniques also available, that we can use in the field of secrete crime detection. The reflection method illuminates the palm using an infrared ray and captures the light given off by the region after spreading through the palm. The presence of deoxidized hemoglobin in the vein vessels absorb the infrared ray, thereby reducing the reflection rate and cause the veins to appear as a black pattern. This vein pattern verified against a preregistered pattern to authenticate the individual. After this comparison we can find out the dissimilarities.

Veins are internal in the body and have a affluence of differentiating features, attempts to forge an identities are extremely difficult, thereby we can maintain a high level of security. The sensors in the palm vein detecting device can only recognize the pattern of an individual's vein.

False acceptance rate is the rate at which someone other than the actual person is falsely recognized. False rejection rate is the rate at which the actual person is not recognized accurately. In palm vein biometrics false acceptance rate is 0.00008% and the false rejection rate is 0.01%. Comparing to other biometrics techniques this will provides 100% accuracy.

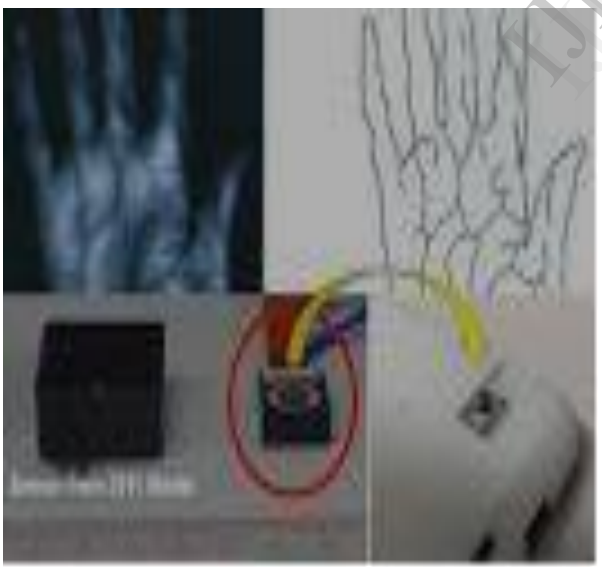

Figure.2. Working of palm vein biometrics

This system is not dangerous; a near infrared is a component of sunlight: there is no more exposure when scanning the hand than by walking outside in the sun. Mainly three steps are involving, that all are,

- Takes snapshot of palm veins
- Create a database of palm vein images
- Converts images into algorithms
- Compare these with database

4. Palm vein authentication and segmentation

Authentication using fingerprints is oldest and the most common biometric technique use nowadays. The ridge patterns on the human fingertip are known to be unique to each individual. For identifying that we use optical, thermal or tactile, electrical scanning to detect the patterns on the finger. Authentication systems measure vein structure, because this also having unique biometric characteristics. Also use an infrared scanning to detect the pattern of veins in a user's finger, palm or the back of the hand. The three main categories of palm matching techniques are,

- Minutiae-based matching
- Correlation-based matching
- Ridge-based matching

Minutiae-based matching is the most widely using technique for palm matching, because it identifies the minute points, specifically the location, direction and orientation of each point. Correlation-based matching involves simply lining up the palm images and subtracting them to determine if the ridges in the two palm images correspond. Ridge-based matching uses ridge pattern landmark features such as sweat pores, spatial attributes, geometric characteristics of ridges, local texture analysis. Compare to these matching methods Minutiae-based matching is faster method for matching and overcomes difficulties associated with extracting minutiae from poor quality images. Procedures followed in palm vein authentication process are,

- Get a palm print image
- Find extraction in input image.
- Apply palm print noisy filter.
- Overlap edge segment
- Get original image as lines
- Get intersecting points.
- Extracted output image.

Segmenting the palm vein video by avoids threshold selection. By avoiding threshold selection we can manage the disturbances of inhomogeneous illumination, low contrast, and noise effectively. The results of segmentation that compare with palm-vein video database built earlier for verification. Compare to latest palm-vein segmentation methods extracting the palm-vein continuously and without selecting thresholds is an efficient way.

5. Video P-frame prediction

Frame prediction is the process of predicting the frames. Prediction is based on current frame predicted from previous frame. Here we bring together an input video from particular mat lab folder.

The prediction error can be compressed at a higher rate than the frames itself, allowing for smaller file sizes. P-picture or P-frame (predictive coded picture) contains motion-compensated divergence information from the previous I- or P-frame.

Imagine an I-frame showing a triangle on white background! A following P-frame shows the same triangle but at another position. Prediction means to supply a motion vector which declares how to move the triangle on I-frame to obtain the triangle in P-frame. This motion vector is part of the MPEG stream and it is divided in a horizontal and a vertical part.

These parts can be positive or negative. A positive value means motion to the right or motion downwards, respectively. A negative value means motion to the left or motion upwards, respectively. Every change between frames can be expressed as a simple displacement of pixels.

6. Frame deletion or addition

This technique identified to increase the video p-frame prediction error. A video forger may wish to add or delete frames from a digital video sequence. To do this, the forger must decompress the video before frames are added or deleted, and then recompress the video after it has been altered.

7. Forensics and anti-forensics

Forensics Technique, detect the use of frame addition or deletion anti-forensics by comparing a compressed videos motion vectors to an estimate of the true motion in the video.

Forensic techniques have been developed to perform a variety of tasks such as detecting evidence of editing or forgery, identifying a media file's origin, and tracing multimedia content's processing. We used forensic algorithms for identifying the palm vein video patterns.

Anti-Forensics Technique**,** remove traces of image resizing and rotation and forge the photo-response non uniformity (PRNU) fingerprint left in an image by a digital camera's electronic sensor .These techniques can be used to fool forensic algorithms that identify image forgeries by searching for inconsistencies in an image's compression. Anti-forensic algorithms are used for identifying the image and detecting if any forgery is occurred among that videos collected before.

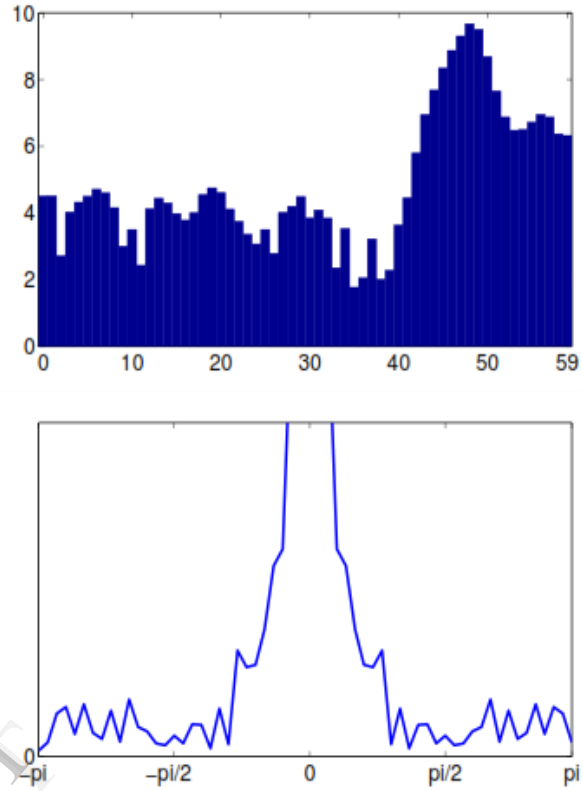

Figure.3. P-frame prediction error sequence (top) and the magnitude of its DFT (bottom)

8. Game theoretical frame work

Game theoretical frame work**,** analyzing the interplay between a forensic investigator and a forger. Game theoretic framework is used for identifying the finest strategies of both the forensic investigator and video forger. In this paper we are considering Many-player game that includes forensic investigator and forger. Some types of game theory are listed here,

- Combinatorial games
- Infinitely long games
- Discrete and continuous games
- Differential games
- Many-player and population games

9. Detecting video forgery

Detection of video forgery is based on threshold value of individual. Detecting video forgery**,** finally we detect an intelligent forger will attempt to modify their anti-forensic operation in order to minimize the strength of their anti-forensic operation. So, that it reduces the strength of the editing operation's palm vein video to just below a forensic investigator's detection threshold.

10. Simulation and results

To evaluate the performance of our proposed anti-forensic technique using palm vein authentication instead of finger prints, we simulated the JPEG compression and decompression process in Matlab and used this to obtain the P-frame prediction error sequence from a number of videos. Fig.3 displaying the prediction error sequence and the magnitude of its DFT. Experimental results demonstrate that our proposed anti-forensic Technique palm vein authentication is capable of removing the temporal palm vein videos from JPEG videos that have undergone frame deletion or addition.

11. Conclusion

In this paper we have proposed palm vein authentication instead of finger prints that use blood vessel pattern as a personal identifying factor for forgery detection. Palm vein pattern authentication technology widely using in Japan and other countries. If this technology is introduced in our country means we can solve password protection in ATM, crimes, anti-forensics techniques, security in various fields and if we implement this technology in government offices we can maintain the work according the government timings. Palm vein authentication technique that creates a tremendous improvement in the field of forensic anti-forensic analysis. Here we can find out a new dimension for anti-forensic techniques by introducing game theory concept in the field of palm vein technology. We surely this technology will bring a revolution in the field of science and technology in the near future.

12. References

[1] M. C. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1050–1065, Sep. 2011.

[2] M.C.StammandK.J.R.Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Trans. Inf. Forensics Security,vol.5,no.3, pp. 492–506, Sep. 2010.

[3] A.Swaminathan,M.Wu,and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 3, no.1, pp. 101–117, Mar. 2008.

[4] M. C. Stamm and K. J. R. Liu, "Anti-forensics for frame deletion/addition in MPEG video," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Prague, Czech Republic, May 2011, pp. 1876–1879.

[5] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Forensics vs. anti-forensics: A decision and game theoretic framework," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Kyoto, Japan, Mar. 2012, pp. 1749–1752.

[6] M. C. Stamm, S. K.Tjoa,W.S.Lin,andK.J.R.Liu, "Undetectable image tampering through JPEG compression anti-forensics," in Proc. IEEE Int. Con f. Image Processing, Sep. 2010, pp. 2109–2112.

[7] M. C. Stamm and K .J.R.Liu, "Wavelet-based image compression anti-forensics," in Proc. IEEE Int. Conf. Image Processing, Sep. 2010, pp. 1737–1740.

[8] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Anti-forensics of JPEG compression," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Mar. 2010, pp. 1694–1697.

[9] M.Goljan, J.Fridrich,andM.Chen, "Defending against fingerprint- copy attack in sensor-based camera identification," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 227–236, Mar. 2011.

[10] I.Avcibas,S.Bayram,N. Memon, M. Ramkumar, and B. Sankur, "A classifier design for detecting image manipulations," in Proc. IEEE Int. Conf. Image Processing, Oct. 2004, vol. 4, pp. 2645–2648.

[11] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Source digital camcorder identification using sensor photo response non-uniformity," in Proc. SPIE Electronic Imaging, Photonics West, Feb. 2007, vol. 6505.

[12] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[13] W. Wang and H. Farid, "Exposing digital forgeries in interlaced and de-interlaced video," IEEE Trans. Inf. Forensics Security,vol.3,no.2, pp. 438–449, Jun. 2007.

[14] W. Wang and H. Farid, "Exposing digital forgeries in video by detecting double MPEG compression," in Proc. ACM Multimedia and Security Workshop,Geneva, Switzerland, 2006, pp. 37–47.

[15] G. Valenzise, V. Nobile, M. Taglisacchi, and S. Tubaro, "Countering JPEG anti-forensics," in Proc. IEEE Int. Conf. Image Processing,Brussels,Belgium,Sep.2011.

[16] Masaki watanabe, Toshio Endoh, Morito Shiohara, and Shigeru Sasaki, "Palm vein authentication technology and its applications," in Proceedings of the Biometric Consortium Conference,Arlington,VA,USA,Sept.2005.

[17] Ishani Sarkar, Farkhod Alisherov, Tai-hoon Kim, and Debnath Bhattacharyya, "Palm vein authentication: A Review," in International Journal of Control and Automation, March. 2010, vol. 3, pp. 27-33.