Video Forgery Detection Using Features Extraction And Segmentation Techniques

Ramasamy V[1], Dinesh Kumar P[2], Sanjay P[3], Senthil Kumar S[4]

[1] Associate Professor, Department of Information Technology, M. Kumarasamy College of Engineering, Karur, Tamilnadu, India

[2,3,4] U.G. Student, Department of Information Technology, M. Kumarasamy College of Engineering, Karur, Tamilnadu, India

Abstract

The ability to edit digital videos is becoming increasingly straightforward as video editing tools progress. Determining the authenticity of videos has become a prominent problem in the area of information security. The purpose of video forensics is to uncover characteristics that distinguish authentic movies from forgeries. As a result, people can tell whether a video is genuine or not. A form of differentiating strategy based on video data that includes copy-move detection and inter-frame manipulation detection has become a hot topic in video forensics. Anyone may now publish, download, and distribute materials such as audio, photographs, and video over the internet thanks to the rise of viruses.Two examples of Multimedia software and tools are programmers that allow you to edit or alter media files are Video Editor and Adobe Photoshop. Furthermore, altering video sequences in such One of the most typical malicious video forging procedures is the insertion or deletion of objects within the frame. In this research, copy move assaults are identified using Detection of video counterfeiting using features taken from frames and compared to authentic footage, and for detection, the Scale Invariant Feature Transform (SIFT) has been improved. First, picture key points are obtained, and a multi-dimensional feature vector known as a SIFT descriptor is created for each key point. These crucial spots are then matched using distance as one of their properties. Despite the fact that this approach detects copy move attacks effectively. We can provide information on the total number of forged frames, as well as the types of forged frames. Create the application as a window-based application using image processing techniques as well.

Index Terms—Forgery of video, Features Extraction, Key points, Query frames, Reference frames, SIFT features

I. INTRODUCTION

Computer forensics (sometimes referred to as computer forensic science) is a subset of digital forensics that deals with evidence acquired from computers and digital storage media. Computer forensics is the forensic examination of digital media with the objective of detecting, conserving, retrieving, analyzing, and presenting facts and perspectives on the digital data. Although computer forensics is most commonly linked with the investigation of a wide range of computer crimes, it can also be used to investigate other types of crimes, it can also be employed in civil lawsuits for other objectives. Although data recovery techniques and concepts are employed, there are additional norms and practices in place to ensure that a legal audit trail is produced.The same concepts and approaches apply to computer forensics evidence as they do to other types of digital evidence. It has been employed in a number of high-profile cases and is slowly gaining acceptance as a trustworthy tool in both the American and European legal systems.

Passive and active recording devices are the most frequent digital video evidence types. A recording system that does not save information in its memory system is referred to as a "passive recording system." A method for active recording saves data by using its memory system. A hard disc drive (HDD), solid state drive (SSD), or volatile (flash) memory is the most common digital storage medium used in active recording systems. Digital video records are created in the following formats by video recorders:

Format for open source:A file format for storing digital data that is defined by a publicly disclosed specification that anyone may use and amend is known as an open-source format. A standards organization is normally in charge of keeping it up to date.

Format that is unique to the company:A proprietary format is a file format used by a firm, organization, or person to store and arrange data using a specific encoding method. This system is intended to be hidden by the company or organization, with only proprietary software or hardware provided by the company being able to decode and interpret the data saved. These formats are becoming more popular because they are a more secure and higher quality format when video evidence is obtained directly from the system that made it. These proprietary formats also include digital data such as Meta Data and Telemetry Data, which can aid in a video forensic investigation.

Format for use in a courtroom:A computer, projection device, or huge television can simply play a duplicate of the video clip in a court of law. Before being presented in court, this digital format should be tested on the computer it will be played on. This format is commonly provided by a flash drive, DVD, or Data Disc. Despite the fact that the watchable copy will be encoded in a standard video format (MP4, AVI, WMV), it may still be necessary to advance frames and smoothly play or decode the movie using a freeware player such as VLC or DVD playing software.A professional video forensic specialist uses scientific methodologies such as forensic video analysis and authenticated video recording to ascertain what happened at the time of the incident. Things are seen differently by the human eye and by CCTV cameras. Some of the video recordings we review in our lab have been tampered with, either deliberately or unintentionally, utilizing methods that compromise the evidence's integrity. As video forensic specialists, we are required to review and conduct several scientific tests in order to determine the nature of any anomalies in the video recording so that we may aid our client attorneys in understanding the anomalies.Because of the widespread availability of digital video and digital picture editing software, accurate multimedia content authentication has become problematic. Thanks to With today's modification techniques and the continuous advancement of multimedia technology, even a novice may quickly delete an object from a video sequence, add an object from another video source, or insert a graphical object. program designer. It's becoming increasingly difficult to

distinguish between a legitimate video and one that has been tampered with. Figure 1 depicts the basic layout forgery detection.

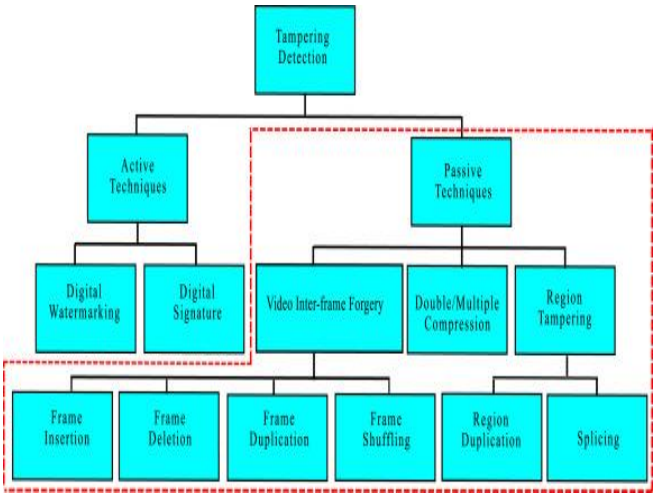

Fig 1: Tampering detection techniques

II. Related Work

MubbasharSaddique, et.al,…[1] This research focused on both recognizing and locating forged video segments (VSs). The texture of micro-patterns in tampered frames is changed during spatial domain video manipulation, which is a major evidence of fraud. To describe tampering traces in video frames, the texture descriptor Histogram of Oriented Gradients (HOG) was used. Gradient orientation is used in this descriptor and its derivatives, despite the fact that it is ineffective in describing local texture micro-patterns and modifications. HOG only provides shape information due to its gradient orientation, making it subject to noise and scale fluctuations. The Local Binary Pattern is another prominent texture descriptor being studied for image counterfeit detection (LBP). It's been utilized for a wide range of categorization tasks. Noise and tiny gray-level fluctuations are vulnerable to this description, which is resistant to monotonic illumination changes and contrast variation. Furthermore, edge strengths are not taken into account by LBP.

Mohammed aloraini, et.al,…[2] installed a surveillance video surveillance system that has become critical for social security and monitoring many organizations, and it is critical to verify the trustworthiness of these surveillance films. If these recorded films are misused, it could result in a slew of serious issues with public safety and legal evidence. That is, determining whether a recorded video is real or not, especially when it is utilized as key evidence in a court of law, is the fundamental challenge. Furthermore, with the emergence of powerful and simple-to-use media editing tools, an attacker might maliciously fabricate a video sequence by adding or deleting an object in a scene with little effort and no obvious traces.This fabricated film is frequently deceptive since it appears realistic and so credible. That is, media are occasionally duped into publishing faked movies as though they were authentic As a result, video footage should be scrutinized properly to ensure its validity and integrity, hence decreasing digital crimes. The topic of identifying object-based video counterfeiting is investigated in this research. Due to the possibility of varied speeds and illuminations in movies, Adding moving objects without leaving visual traces is tricky. We offer a method for detecting and estimating the movement of eliminated moving objects from a video scene captured by a static camera. Object-based video forgeries are examined in this work, and a method based on it is proposed.We also demonstrated that using spatial decomposition and sequential analysis, the suggested approach can estimate the movement of different sizes of removed objects and detect temporal changes that are practically imperceptible. Our method not only surpasses the other in terms of Precision, Recall, and F1 score, but it is also more resilient against compressed and lower definition films, according to the results. Because the sequential analysis stage is computationally expensive, we will focus our future research on enhancing the detection speed of the suggested technique.

Mengnan du, et.al,…[3]have been committed to detecting forgeries, their detection generalization capability remains an issue, and their performance reduces dramatically on previously unknown but comparable manipulations. To close this gap, we offer the Locality-aware Auto Encoder (LAE) in this research, which integrates In a single framework, fine-grained representation learning and locality enforcement are combined. We use pixel-wise mask to regularize local interpretation of LAE to encourage the model to learn intrinsic representation from the forgery region, rather than collecting artifacts in the training set and learning spurious correlations to achieve detection.We also offer an active learning system for identifying the most difficult candidates for labeling and reducing annotation efforts to ensure consistency in interpretations. The results of the experiments show that LAE can make decisions by focusing on the forgery sections. The results also reveal that LAE outperforms In terms of universality, state-of-the-arts on forgeries developed by various manipulation methodologies.Based on the foregoing discoveries, we provide the Locality-aware Auto Encoder (LAE) in this paper for improved forgery detection generalization. LAE considers both fine-grained representation learning and enforcing locality in a single framework for image forensics. Our method is based on an auto encoder that captures the distribution for the training images using reconstruction losses and latent space loss, resulting in fine-grained representation learning. To regularize the local interpretation, we add local interpretability to the auto encoder and use extra pixel-wise forgery ground

truth to defend against false correlations learnt by the auto encoder. As a result, the LAE is enforced in the forgery region to catch discriminatory representations.

Irene amerini, et.al,…[4] Deep learning techniques are increasing the technological sophistication of multimedia content creation and processing. Deep Fakes (DF) is a new phenomenon that allows people to easily create realistic videos in which their faces, or sometimes just their lips and eyes movements, are altered to likely simulate the presence of another subject in a given context or to make someone speak coherently with a different and, most likely, compromising speech.When this false information is used to intentionally injure a person, such as a public personality or a politician, or even an organization, such as a political party, the consequences are obvious. The impact of Deep Fakes can also be enhanced by social media's ability to distribute information swiftly and globally. According to this, the machine learning community has paid special attention to this phenomenon in two ways. This extended abstract provides a revolutionary technique for identifying real from deep fake-like films. In contrast to state-of-the-art algorithms that normally operate in a frame-based manner, we offer a sequence-based technique dedicated to analyzing possible dissimilarities in the temporal structure of a video.Specifically, optical flow fields were collected in order to take advantage of inter-frame correlations and feed them into CNN classifiers. The idea of using This work introduces and investigates optical flow field dissimilarities as a cue to discern between deep fake and legitimate videos. This is a rather inventive way of accounting for possible temporal inconsistencies in the sequence. Motion vectors were represented as 3-channel images in this first experiment, and then used as input for a neural network to overcome the challenge of using a pre-trained network.

Markoszampoglou, et.al,…[5] There is a pressing demand for tools to help professionals detect and prevent manipulated content. Multimedia forensics attempts to bridge this gap by developing techniques and tools that assist investigators in detecting traces of manipulation and extracting information about the history of a multimedia item. In recent years, research into automatic video verification has progressed tremendously; nonetheless, state-of-the-art systems are not yet mature enough for journalists without specialized training to utilize. Expert verification, or skilled specialists visually inspecting the film under several picture maps (or filters4) in order to find inconsistencies, is now the most common method used in real-world video forensics. We investigate the possibility of two unique filters developed for human visual assessment in the context of automatic verification in this article. The filter outputs are used to train a collection of deep learning visual classifiers to learn to discriminate between real and manipulated videos. We examine their viability in real-world scenarios using a dataset of well-known tampered and unhampered news-related videos from YouTubescenarios, in addition to proven experimental forensics datasets.

III. EXISTING METHODOLOGIES

Wang,W.[11] The cheap availability of video and image altering software has made it harder to authenticate multimedia information in recent years. Signal acquisition and processing thanks to the availability of has been more accessible to a wider range of people low-cost and easy-to-use digital multimedia equipment (such as digital cameras, mobile phones, digital recorders, and so on), as well as high-quality data processing tools and algorithms. As a result, a single image or video can be processed and changed by multiple people. Because the originality and integrity of digital content cannot be guaranteed, this fact has serious ramifications when it is used to support legal evidence.Important elements in the recorded scene might be buried or removed, and the genuine source of the multimedia material can be hidden. Furthermore, because there is no method to identify the original owner, detecting copyright infringements and validating the legal possession of multimedia data may be challenging. Illegal crimes are committed using digital movies and photos with fake material. As a result, the integrity of digital content must be validated. Analyzing the qualities of digital media can help with this. The current method separates the test video is divided into frames, with each frame divided into 12 non-overlapping sub-blocks. Each sub-block is translated into each frame the frequency domain using the discrete cosine transform (DCT). Each sub-average block's DCT value is Each frame is calculated, and a row vector containing averaged DCT values is obtained. For each frame, the generated row vectors are binarized. By computing a correlation matrix utilizing binary row vectors, the suggested technique creates a correlation image for the current test video. In the correlation image, brighter pixels represent similar frames.

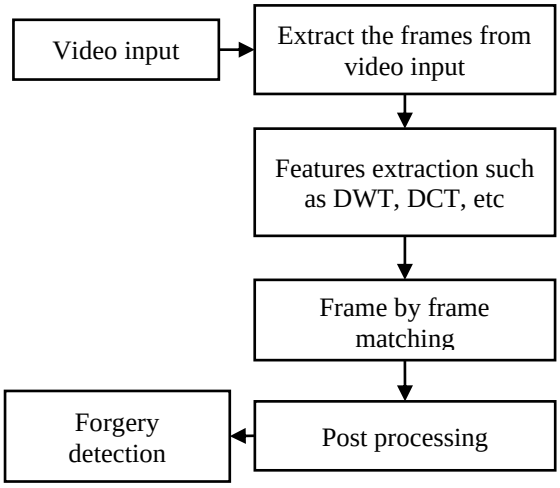

Fig 2: Existing approaches2 depicts the present framework

IV. PROPOSED METHODOLOGY

Shivakumar, B. L., [12] Our daily lives are now pervaded by digital video material as one of the most significant ways of communication in the digital era. People and society have benefited from advances generation, transmission, storage, and retrieval of video, as well as applications such as video sharing platforms and video conferencing. Images and videos on video sharing and social networking sites like YouTube, Facebook, Instagram, and others are emblematic of social, economic, and scientific development. Other applications, such as the entertainment industry, video surveillance, legal evidence, political videos, video courses, advertisements, and so on, show how revolutionary they are in today's world. Videos may be quickly made, stored, sent, and processed in digital format because to the widespread use of the Internet, as well as inexpensive and high-quality cameras, PCs, and user-friendly editing tools.Any inexperienced person can use these approaches to make unlawful changes to video content, compromising its integrity and authenticity. This option necessitates determining whether multimediaImage and Video Source Class Identification [13] content retrieved via The information on the internet, as part of a video surveillance system, or as received by a broadcaster is authentic. As a result, there is a dark side to videos, which is the misapplication or incorrect projection of information through videos, in addition to its amazing behavior. The purposeful modification or alteration of a digital video for the purpose of fabrication is known as digital video forgery. Video forgeries are the manipulation of a video in such a way that the content is perceptually altered.Video falsification can range from simple things like inserting advertising into sporting event broadcasts to more complicated things like digitally removing people from a video. The two categories of video forgeries are spatial forgeries and temporal forgeries. When collecting a video sequence, there is frequently a lot of redundancy between the successive frames. The MPEG video compression method takes advantage of this redundancy by anticipating particular frames in a video sequence and storing the difference between the expected and actual frames. This results in a more efficient compression strategy since the expected difference may be compressed at a faster rate than the entire frame Compression, on the other hand, has issues with this approach since any inaccuracy introduced by one frame propagates to all frames predicted from it. To prevent error propagation, the video sequence is divided into segments, each of which is referred to as a group of photographs (gop). To prevent decoding difficulties from spreading across the video sequence, frame prediction is performed inside each segment, but not across segments.Within each group of images, there are three types of frames: intra-frames (I-frames), predicted-frames (P-frames), and bidirectional-frames (B-frames). Each cycle begins with an I-frame and continues through P-frames and B-frames. Because no prediction is done when encoding I-frames, each one is encoded and decoded sequentially. During encoding, each I-frame is compressed using a loss algorithm similar to JPEG [14] compression.Motion estimation is used to encode P-frames in a predictive fashion. SIFT characteristics are retrieved from gray-level images and are generally insensitive to post-processing techniques. They're employed in a wide range of image processing applications, from medical to space-related. It is the most commonly researched algorithm, with a variety of modified variations.

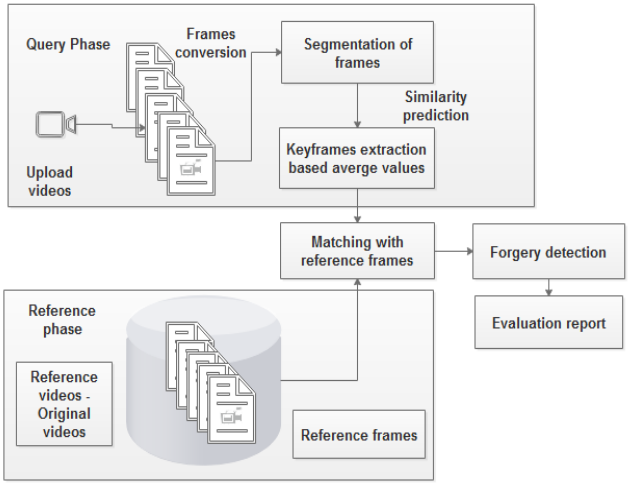

Fig 3: Proposed framework

VIDEO ACQUISITION:

We can upload videos that are deemed inquiry videos in this module. Original videos, sometimes known as reference videos, are available to the administrator. Using video file reader coding, we can transform the videos into frames every 0.5 seconds. Each frame is treated as a separate image.

VIDEO FEATURES EXTRACTION:

The practice of reducing the resources required to explain a large quantity of data is known as feature extraction. The vast number of variables involved is one of the most difficult aspects of conducting extensive data analysis. Feature extraction is a broad term that relates to methods for combining variables to avoid these problems while still accurately describing the data. We may extract features from each frame in this module, such as color, object form, background features, and so on. These characteristics are extracted in order to perform future integrity checks.

SEGMENTATION OF VIDEOS:

Segmentation is the process of grouping frames based on video characteristics. Video segmentation is a technique for separating frames into meaningful chunks. Segmentation is best used in the context of video capture to capture a screen presentation that the presenter goes through slide by slide. Detection offrame [15] and the program compares and calculates

the similarity of each video frame in order to determine whether or not the scenery has changed. We'll break the video here if there's a change, and then we'll break it into shots. We consider the first frame of each shot to be the crucial frame and show it to the users. To compare the similarity of two video frames, we use the Color Indexing concept. Key frames are retrieved and saved as segmented frames in this module.

VIDEO FRAMES CLASSIFICATION:

Following segmentation, we can get a list of feasible frames that are less than the total number of video frames. The query video segmented frames are matched with the reference video segmented frames in this module. Both frames are used to determine similarity values. These figures are derived from each frame's color, shape, and texture data.

FORGERY PREDICTION:

If the similarity values aren't the same, the video should be regarded as a counterfeit. Otherwise, take the values as they were. Predict the forgery frames from inquiry videos if it's forgery.

V. EXPERIMENTAL RESULTS

The proposed work can be implemented as Video forgery detection framework using C#.NET as front end and SQL SERVER as back end. Based on proposed algorithm we can detect the forgery pixels in uploaded videos. The performance of the proposed system can be evaluated in term of time in seconds. In this screen, display the features matching for original Every crucial point can benefit from videos and similarity matching. The original videos are displayed on the screen.

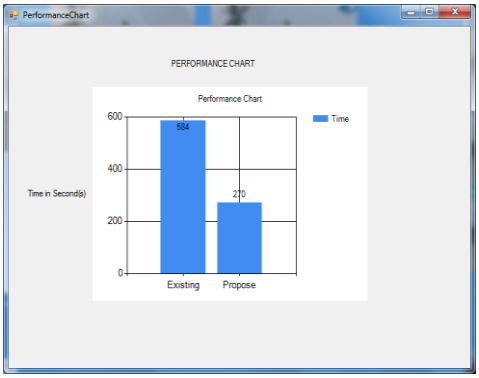

Fig 4: Performance chart

The system's performance can be measured in terms of time. In comparison to the present framework, the suggested framework examines forgeries frames in a fraction of the time.

VI. CONCLUSION

By recovering information about a video's history, digital video forensics tries to verify its validity. Copy paste forgery is when a segment of a video is changed with a segment from another video (with possible transformations). Because the cloned segment is Significant aspects like noise, color palette, and texture from the same video will blend in with the rest of the movie, making it more difficult to recognize and detect. The purpose of video copy detection is to provide an automated video analysis tool for copyright control, monitoring, and database structuring that can recognize original and modified copies of a video amid a large amount of video data. Video on the internet forensics is a relatively young branch of study that tries to verify the authenticity of videos by retrieving information about their past. Natural, forgery detection, flow mapping, and source identification are the four fundamental difficulties identified by studies in the literature. As a result, determining the originality and validity of movies or data has become a difficult task in many circumstances. We offer various novel digital forensic approaches in this research to detect indications of editing in digital multimedia information. For forensic tasks like cut-and-paste forgeries from JPEG compressed movies and SIFT, we apply segmentation-based forgery detection. This SIFT-based approach relies on key point detection for feature extraction. If there is an occurrence of duplicate move attack, this method is most commonly applied to locate vengeful control with computerized records (advanced frauds). The planned effort has yielded a viable result in the form of a correlation with the leaving model.

VII. FUTURE SCOPE

In future, effective research is required toCopy paste forgery is when a segment of a video is changed with a segment from another video. Also we can reduce a time and accuracy of the video in the application. The video forgery can be easily identified Using future techniques.

REFERENCES

[1] Aloraini, Mohammed, et al. "Statistical sequential analysis for object-based video forgery detection." Electronic Imaging 2019.5 (2019): 543-1.

[2] Du, Mengnan, et al. "Towards generalizable forgery detection with locality-aware autoencoder." arXiv preprint arXiv:1909.05999 (2019).

[3] Amerini, Irene, et al. "Deepfake video detection through optical flow based cnn." Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops. 2019.
[4] Zampoglou, Markos, et al. "Detecting tampered videos with multimedia forensics and deep learning." International Conference on Multimedia Modeling. Springer, Cham, 2019.
[5] Saddique, Mubbashar, et al. "Spatial video forgery detection and localization using texture analysis of consecutive frames." Advances in Electrical and Computer Engineering 19.3 (2019): 97-108.
[6] Kannadhasan Suriyan, Nagarajan Ramalingam, Sundarmani Rajagopal, Jeevitha Sakkarai, Balakumar Asokan, Manjunathan Alagarsamy, Performance Analysis of Peak Signal-to-Noise Ratio and Multipath Source Routing Using Different Denoising Method, Bulletin of Electrical Engineering and Informatics, Vol.11.No.1, February 2022, pp.286-292, ISSN No:2302-9285, DOI: 10.11591/eei.v11i1.3332
[7] Stütz, Thomas, FlorentAutrusseau, and Andreas Uhl. "Non-blind structure-preserving substitution watermarking of H. 264/CAVLC inter-frames." IEEE Transactions on Multimedia 16.5 (2014): 1337-1349.
[8]Kot, A. C., & Cao, H. (2013). Image and Video Source Class Identification. In Digital Image Forensics (pp. 157-178). Springer New York.
[9]Shanableh, T. (2013). Detection of frame deletion for digital video forensics. Digital Investigation, 10(4), 350-360.
[10] R.Bharathi, T.Abirami," Energy efficient compressive sensing with predictive model for IoT based medical data transmission", Journal of Ambient Intelligence and Humanized Computing, November 2020, https://doi.org/10.1007/s12652-020-02670-z
[11]Shivakumar, B. L., & Santhosh Baboo, L. D. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. Global Journal of Computer Science and Technology, 10(7).
[12] Mol, Jacob Jan-David, et al. "The design and deployment of a bittorrent live video streaming solution." 2009 11th IEEE International Symposium on Multimedia. IEEE, 2009, DOI-10.1109/ISM.2009.16
[13] Thouin, Frederic, and Mark Coates. "Video-on-13emand networks: design approaches and future challenges." IEEE network 21.2 (2007): 42-48.
[14] Wang, W. (2009). Digitalvideo forensics (Doctoral dissertation, Dartmouth College Hanover, New Hampshire).
[15]Suhail, M. A., &Obaidat, M. S. (2003). Digital watermarking-based DCT and JPEG model. Instrumentation and Measurement, IEEE Transactions on, 52(5),1640-1647, DOI: 10.1109/TIM.2003.817155