ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

Detection of Malicious Attack in Digital Video Using Watermarking

M.Mageshbabu [1], V.G.Vengatesan[2], P.G.Karthikeyan[3]

Assistant Professor, Department of Electronics and Communicaton Engineering, SKP Engineering College

Tiruvannamalai, Tamilnadu, India[1, 2, 3]

ABSTRACT: We present our project to distinguish malicious attack from common processing operation such as recompression, noise and brightness increasing using practical watermarking scheme. Analysis of the error is used to detect tampering. A well-known solution to the above problems are watermarking, which hides important information in the media. A well-designed watermarking system must provide three main features such as transparency, robustness and capacity. To apply data hiding to content authentication, a semi fragile watermarking technique could be considered to tolerate certain kinds of processing, such as recompression and at the same time detect malicious tampering manipulation. We verify our performance by simulation using MATLAB. Additionally,the following algorithms used in our paper are DCT (discrete cosine transform), DFT (discrete wavelet transform), HEVC (high-efficiency video coding) and DWT (discrete wavelet transform) H.264/AVC.The Main advantage of our project is content- based cryptography and increases the security of the system. The applications of our project are military purpose, government work and security purpose.

KEYWORDS: Video authentication, video tampering detection, video watermarking,Data hiding.

I.INTRODUCTION

The introduction of watermarking and the related publications date back to 1979. However, it was only in 1990 that it gained large international interest. Digital watermarking involves embedding watermark data into original information. In other words, a watermark is a pattern of bits inserted into multimedia data such as digital image, audio or video file that helps to identify the file's copyright information (author, rights, etc.). A simple example of a digital watermark may be a visible signature or seal placed over an image to determine the owner of that image. The name "watermark" is derived from the faintly visible marks imprinted on organizational stationery. Unlike printed watermarks, which are intended to be somewhat visible, digital watermarks are designed to be completely invisible, or in the case of audio clips, inaudible. In addition, the bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. The embedding technique must keep the original information perceptually unchanged and the watermark data should be detected by an extraction algorithm.

In recent years, the advances in communication technology have seen strong interest in digital image transmission. However, growth of computer processor possessing power and storage illegal access has become easier. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code, scientific community have seen strong interest in image transmission.

However, illegal data or image access has become more easy and prevalent in wireless and general communication networks. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption / decryption is essential, furthermore. As such in this paper, a scheme based on encryption has been proposed for secure image transmission over channels.

Digital images, accounting for 70% of the information transmission on the internet, is an important parts of network exchanges. However, the image information, which is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels.

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

Traditional encryption algorithms such as DES, IDES, are against the text messages to be proposed, which are not suitable for digital image encryption, therefore, an reliable digital image with characteristics is in urgent need of the encryption scheme AES is suitable for image encryption, and decryption with is closely related to some dynamics of its own characteristics.

II.PROPOSED WATERMARKING SCHEME

Load video and convert rgb image to YCBCR,from this take only Y component. Then apply dct to each frame.After performing DCT and the quantization phases, some 4 × 4 blocks of each 16 × 16 MB are selected for embedding. With the number of secret bits which will be embedded into an MB, the number of selected blocks is chosen. In each MB, the blocks that have larger LNZ level position are selected, i.e., blocks that have the highest high frequency sample. Choosing high-frequency QDCT values imposes lower modification distortion. In each selected block, a single secret bit is embedded. If the corresponding secret bit is zero, the sum of all levels should be even. If it is odd, the LNZ level is incremented or decremented by one. If the secret bit is one, the sum should be odd. However, if the sum is even, the LNZ level should be incremented or decremented by one. For increased robustness, we also use some other nonzero levels, though at a tradeoff with increased distortion.

DIGITAL WATERMARKING.

In generally digital watermarking is a technique for inserting information into an image. It is an evolving field that requires continuous effort to find the best possible method in protecting multimedia content. It is a process of embedding information into digital multimedia content such that the information can later be extracted or detected for variety of purposes including identification and authentication.

RGB COLOR IMAGE**:**

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. The name of the model comes from the initials of the three additive primary colors, red, green, and blue.

GRAYSCALE:

In photography and computing,a grayscale or grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest.

Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only the two colors, black, and white (also called bi-level or binary images). Grayscale images have many shades of gray in between. Grayscale images are also called monochromatic, denoting the presence of only one (mono) color (chrome).

Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum (e.g. infrared, visible light, ultraviolet, etc.), and in such cases they are monochromatic proper when only a given frequency is captured. But also they can be synthesized from a full color image; see the section about converting to grayscale.

ADAPTIVE HISTOGRAM EQUALIZATION

Histogram equalization is a method in image processing of contrast adjustment using the image's histogram.

This method usually increases the global contrast of many images, especially when the usable data of the image is represented by close contrast values. Through this adjustment, the intensities can be better distributed on the histogram.

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

This allows for areas of lower local contrast to gain a higher contrast. Histogram equalization accomplishes this by effectively spreading out the most frequent intensity values.

The method is useful in images with backgrounds and foregrounds that are both bright or both dark. In particular, the method can lead to better views of bone structure in x-ray images, and to better detail in photographs that are over or under-exposed. A key advantage of the method is that it is a fairly straightforward technique and an invertible operator. So in theory, if the histogram equalization function is known, then the original histogram can be recovered. The calculation is not computationally intensive. A disadvantage of the method is that it is indiscriminate. It may increase the contrast of background noise, while decreasing the usable signal.

THRESHOLDING

Thresholding is the simplest method of image segmentation. From a grayscale image, thresholding can be used to create binary images.

Categorize thresholding methods into the following six groups based on the information the algorithm manipulates.

- Histogram shape-based methods, where, for example, the peaks, valleys and curvatures of the smoothed histogram are analyzed
- Clustering-based methods, where the gray-level samples are clustered in two parts as background and foreground (object), or alternately are modeled as a mixture of two Gaussians
- Entropy-based methods result in algorithms that use the entropy of the foreground and background regions, the cross-entropy between the original and binarized image, etc.
- Object Attribute-based methods search a measure of similarity between the gray-level and the binarized images, such as fuzzy shape similarity, edge coincidence, etc.
- Spatial methods [that] use higher-order probability distribution and/or correlation between pixels
- Local methods adapt the threshold value on each pixel to the local image characteristics.

COMPRESSION

Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. Lossy compression methods, especially when used at low bit rates, introduce compression artifacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The lossy compression that produces imperceptible differences may be called visually lossless.

GENERAL FRAMEWORK FOR WATERMARKING

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be **detected** or **extracted** later to make an assertion about the object. The object may be an **image** or **audio** or **video**.

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

ENCODING PROCESS: The Fig. 1.1 illustrates the encoding process.

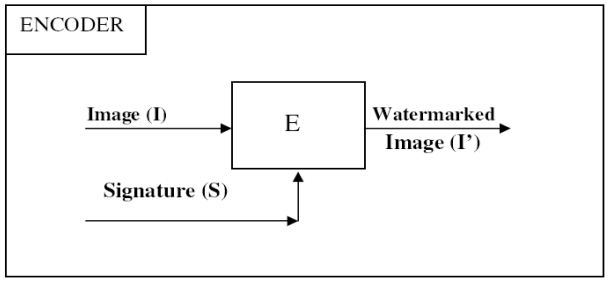


Fig. 1.1 Encoder

. } the watermarked image by I'. E is an encoder image which is called watermarked image I', i.e.

on image I. In such cases, the encoding process

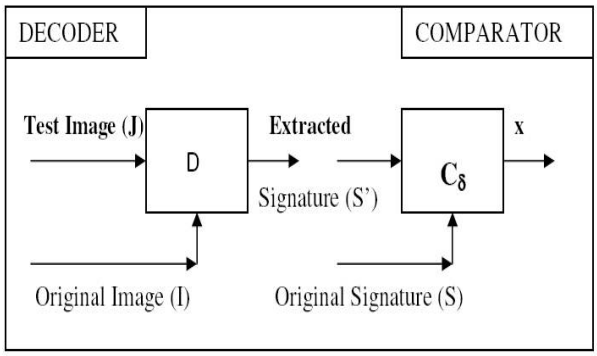


Fig. 1.2 Decoder

A decoder function D takes an image J (J can be a watermarked or unwatermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature S' from the image. In this process, an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D(J, I) = S' \qquad (1.2)$$

The extracted signature S' will then be compared with the owner signature sequence by a comparator function Cd and a binary output decision generated. It is 1 if there is a match and 0 otherwise.

$$Cd(S', S) = \begin{cases} 1, & c >= d \\ 0, & \text{otherwise} \end{cases} \qquad (1.3)$$

Here, c is the correlation of two signatures and is certain threshold. Fig1.3 shows the comparator.

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

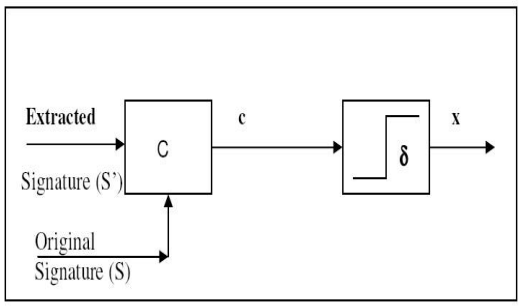
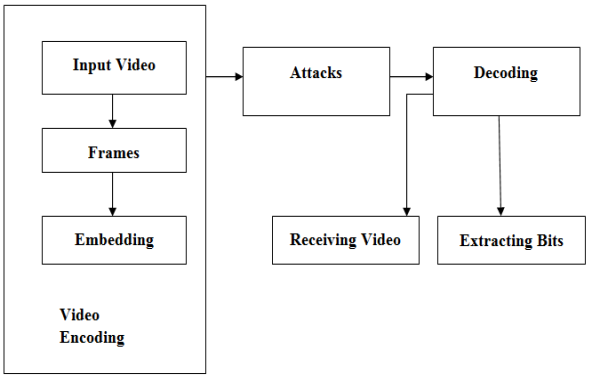


Fig. 1.3 Comparator

Where C is the correlator and x = Cd(S', S). Without loss of generality, watermarking scheme can be treated as a three-tuple (E, D, Cd).

A watermark must be detectable or extractable to be useful . Depending on the way the watermark is inserted and depending on the nature of the watermarking algorithm, the method used can involve very distinct approaches. In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call watermark extraction. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call watermark detection. It should be noted that watermark extraction can prove ownership whereas watermark detection can only verify ownership.

OVER ALL DIAGRAM:



MODULE NAMES

1. Input video & frame conversion
2. Embedding
3. Attacks
4. Decoding
5. Performance analysis

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

MODULE DESCRIPTIONS:

INPUT VIDEO & FRAME CONVERSION:

Take sample input video and converted into frames. video frames is modulated into the parameters of a chaotic system. Then, the output chaotic stream is used as watermark and embedded into the block-based DCT domain of video frames.

EMBEDDING:

Here we embed only binary data's (combination on 1's & 0's). For embedding we use DCT and pseudorandom number generators are used. The index of each MB is embedded inside of it; also, the index of each frame is embedded into the current frame. Thus, this scheme provides a good solution for both spatial and temporal tampering. H.264/AVC recompression, noise, filtering, and other spatial changes cause some errors in tamper detection. However, in our scheme, analyzing the extraction error will distinguish malicious attacks from common processing, such as compression. In addition, extracted frames' indices help us to recognize any frame manipulation, such as adding extra frames, reordering, dropping, or replacement of video frames.

ATTACKS:

Attacks may be like Gaussian noise, salt and pepper noise and brightness increase. Attacks may include additive noise, resizing, low-pass filtering, and any other attack, which may remove the watermark or confuse the watermark extraction system. The attacker needs to have both the original and marked video to find the modified QDCT values. This is highly unlikely that an attacker can access the original video to discover the changes.

DECODING:

Do the reverse process of embedding we get extracted secret bits and extracted image. The embedded watermark bits are extracted in the video decoding process where the quantized DCT levels for each MB are entropy decoded.

PERFORMANCE ANALYSIS:

PSNR , SSIM and bitrate are used for performance evaluation. PSNR is a very popular and widely used evaluation method, it is known that its correlation to subjective quality measures is not always good, because it reflects only the luminance component and neglects the chrominance component which is important to human perception. Therefore, in addition to PSNR, we have also used the structural similarity index (SSIM) [38], which is a more advanced measurement index. While PSNR measures errors between the original and marked image, SSIM measures the structural distortion, luminance, and contrast differences between the two frames.

TECHNIQUE USED:

Tamper Detection is the ability of a device to sense that an active attempt to compromise the device integrity or the data associated with the device is in progress; the detection of the threat may enable the device to initiate appropriate defensive actions.

MATLAB (**mat**rix **lab**oratory) is a numerical computing environment and fourth-generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and Fortran.

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems.

In 2004, MATLAB had around one million users across industry and academia. MATLAB users come from various backgrounds of engineering, science, and economics. MATLAB is widely used in academic and research institutions as well as industrial enterprises.

MATLAB was first adopted by researchers and practitioners in control engineering, Little's specialty, but quickly spread to many other domains. It is now also used in education, in particular the teaching of linear algebra and numerical analysis, and is popular amongst scientists involved in image processing. The MATLAB application is built around the MATLAB language. The simplest way to execute MATLAB code is to type it in the Command Window, which is one of the elements of the MATLAB Desktop. When code is entered in the Command Window, MATLAB can be used as an interactive mathematical shell. Sequences of commands can be saved in a text file, typically using the MATLAB Editor, as a script or encapsulated into a function, extending the commands available.

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

III .DISCRETE WAVELET TRANSFORM

The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. In other words, this transform decomposes the signal into mutually orthogonal set of wavelets, which is the main difference from the continuous wavelet transform (CWT), or its implementation for the discrete time series sometimes called discrete-time continuous wavelet transform (DT-CWT).The wavelet can be constructed from a scaling function which describes its scaling properties. The restriction that the scaling functions must be orthogonal to its discrete translations implies some mathematical conditions on them which are mentioned everywhere e. g. the dilation equation

$$\phi(x) = \sum_{k=-\infty}^{\infty} a_k \phi(Sx - k).$$

where S is a scaling factor (usually chosen as 2). Moreover, the area between the function must be normalized and scaling function must be ortogonal to its integer translates e. g.

$$\int_{-\infty}^{\infty} \phi(x)\phi(x+l)dx = \delta_{0,l}$$

After introducing some more conditions (as the resstrictions above soes not produce unique solution) we can obtain results of all this equations, e. g. finite set of coefficients a_k which define the scaling function and also the wavelet. The wavelet is obtained from the scaling function as

$$\psi(x) = \sum_{k=-\infty}^{\infty} (-1)^k a_{N-1-k} \psi(2x - k)$$

where N is an even integer. The set of wavelets than forms an orthonormal basis which we use to decompose signal. Note that usually only few of the coefficients a_k are nonzero which simplifies the calculations.There are several types of implementation of the DWT algorithm. The oldest and most known one is the Malaat (pyramidal) algoritm. In this algorithm two filters - smoothing and non-smoothing one are constructed from the wavelet coefficients and those filters are recurrently used to obtain data for all the scales. If the total number of data D=2^N is used and signal length is L, first D/2 data at scale L/2^(N-1) are computed, than (D/2)/2 data at scale L/2^(N-2), ... etc up to finally obtaining 2 data at scale L/2. The result of this algorithm is an array of the same length as the input one, where the data are usually sorted from the largest scales to the smallest ones.Similarily the inverse DWT can reconstruct the original signal from the wavelet spactrum. Note that the wavelet that is used as a base for decomposition can not be changed if we want to reconstruct the original signal, e. g. by using Haar wavelet we obtain a wavelet spectrum; it can be used for signal reconstruction using the same (Haar) wavelet.

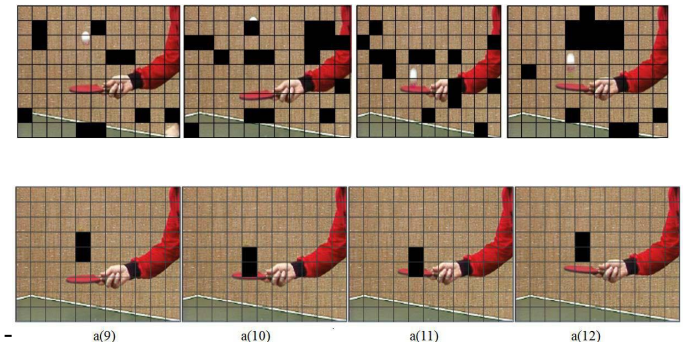
ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

APPLICATION:



Figs.6 and 7 show is that the meaning of thedata is important. In other words, sparse binary errors are affected by some processing that do not change the meaning of the media. However, changes in specific parts of frames show malicious attacks.

IV .SIMULATION RESULT:

ORIGINAL IMAGE

YCBCR IMAGE

ISSN(Online) : 2319-8753

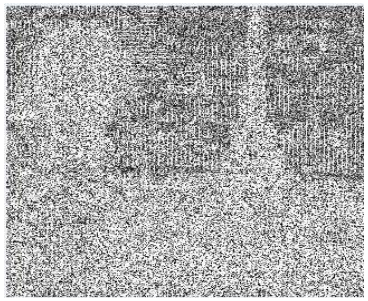
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

Y IMAGE

ENCRYPTED IMAGE



RECOVERED RGB IMAGE

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2013

V. CONCLUSION

In this paper Additionally,the following algorithms used are DCT (discrete cosine transform), DFT (discrete wavelet transform), HEVC (high-efficiency video coding) and DWT (discrete wavelet transform) H.264/AVC.The Main advantage of our project is content- based cryptography and increases the security of the system. The applications of our project are military purpose, government work and security purpose.

REFERENCES

[1] S. Chen and H. Leung, "Chaotic watermarking for video authentication in surveillance applications," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 5, pp. 704–709, May 2008.
[2] P.-C. Su, C.-S. Wu, I.-F. Chen, C.-Y. Wu, and Y.-C. Wu, "A practical design of digital video watermarking in H.264/AVC for content authentication," *Signal Process, Image Commun.*, vol. 26, nos. 8–9, pp. 413–426, Oct. 2011.
[3] D. Xu, R. Wang, and J. Wang, "A novel watermarking scheme for H.264/AVC video authentication," *Signal Process., Image Commun.*, vol. 26, no. 6, pp. 267–279, 2011.
[4] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 43–55, Mar. 2006.
[5] J. Sang and M. S. Alam, "Fragility and robustness of binary phaseonly filter based fragile/semi-fragile digital image watermarking," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 3, pp. 595–606, Mar. 2008.
[6] M. Fallahpour, M. Semsarzadeh, S. Shirmohammadi, and J. Zhao, "A realtime spatio-temporal watermarking scheme for H.264/AVC," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, Minneapolis, MN, USA, May 2013, pp. 872–875.
[7] K. S. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 10, pp. 1499–1512, Oct. 2009.
[8] T. Wiegand, G. J. Sullivan, G. Bjntegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.
.[9] Y. Shi, M. Qi, Y. Yi, M. Zhang, and J. Kong, "Object based dual watermarking for video authentication," *Int. J. Light Electron Opt.*, vol. 124, no. 19, pp. 3827–3834, 2013.
[10] D. K. Zou and J. A. Bloom, "H.264/AVC stream replacement technique for video watermarking," in *Proc. IEEE ICASSP*, Las Vegas, NV, USA, Apr. 2008, pp. 1749–1752.
[11] S. K. Kapotas and A. N. Skodras, "Real time data hiding by exploiting the IPCM macroblocks in H.264/AVC streams," *J. Real-Time Image Process.*, vol. 4, no. 1, pp. 33–41, Mar. 2009.