International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Video Steganography Schema based on AES Algorithm and 2D Compressive Sensing

B. Janapriya

Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, Tamil Nadu, India

ABSTRACT

This paper proposes a novel reversible image data hiding (RIDH) scheme over encrypted domain. The data embedding is achieved through a public key modulation mechanism, in which access to the secret encryption key is not needed. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and non encrypted image patches, allowing us to jointly decode the embedded message and the original image signal. Compared with the state-of-the-arts, the proposed approach provides higher embedding capacity, and is able to perfectly reconstruct the original image as well as the embedded message. Extensive experimental results are provided to validate the superior performance of our scheme.

Keywords : AES, Video Steganography, 2D, Compressive Sensing, RIDH, SVM, 3D, Digital watermarks

I. INTRODUCTION

Steganography or Image processing is a method to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it [1]. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image. Nowadays, image processing is among rapidly growing technologies. It forms core research area within engineering and computer science disciplines too [2] [3] [4].

Image processing basically includes the following three steps:

- Importing the image via image acquisition tools;
- Analyzing and manipulating the image;
- Output in which result can be altered image or report that is based on image analysis.

II. METHODS AND MATERIAL

Digital Watermarking

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal "Watermarking" is the process of hiding digital information in a carrier signal the hidden information should, but does not need to contain a relation to the carrier signal [5]. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional physical watermarks, digital watermarks are often only perceptible under certain conditions, i.e. after using some algorithm. If a digital watermark distorts the carrier signal in a way that it becomes easily perceivable, it may be considered less effective depending on its purpose [6]. Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time [7]. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. A distinguishing mark impressed on paper during manufacture; visible when paper is held up to the light (e.g. $ Bill). Digital Steganography is an extension of Steganography concept in the digital world. A digital watermark is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.).

VisibleSteganography

Invisible steganography

Steganography

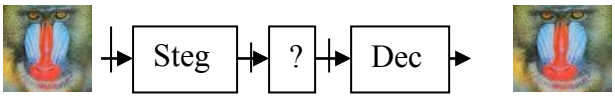
Steganography is changing the digital media in a way that only the sender and the intended recipient is able to detect the message sent through it.

Cover video+hidden data+stego key=stego

The main goal of steganography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot detect the presence of m in d'.Almost all digital file used for steganography but that are not suitable with a high degree of redundancy. The object of those bits can be altered without alteration detected easily. Video and image can be used for information hiding [8].

Cryptography Vs Steganography

Cryptography is the most common method of protecting digital content and is one of the best developed science. The main goal of Cryptography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot remove or replace m in d' However, Steganography cannot help the seller monitor how a legitimate customer handles the content after decryption. Digital Steganography can protect content even after it is decrypted.



Related Work:

A double-image Steganography scheme was existing system based on logistic map and discrete fractional random transform. Where the image was compressed using the lossless image compression scheme as well as it was Watermarked using the chaotic algorithm which was mostly used by so many system currently.

METHOD	ADVANTAGE	DISADVANTAGE
Wavelength coefficient	High Compression Ratio, State of Art	Quantization Bit Allocation
JPEG	Current Standard	Coefficient quantization, Bit allocation
VQ	Simple decoder, No coefficient quantization	Slow codebook generation, Small image

The problem mostly contain the steganography algorithms did not consider image compression or data compression, thus they cannot realize compression and steganography simultaneously. The high end to end delay for overall compression process.

Advanced Encryption Standard (AES):

The AES algorithm is used in the proposed system of the video Steganography process and it is used for securing sensitive data. It has been adopted by the United States government as an Advanced Steganography Standard, a standard algorithm used to Watermark and decrypt sensitive information. AES is a symmetric block cipher with a block size of 128 bits. It allows for three different key lengths which can be 128 bits, 192 bits, or 256 bits; referred to as AES- 128, AES-192, and AES-256, respectively. The number of rounds in the Steganography process for AES-128 is 10, for AES-192 it is 12, and for AES-256 it is 14.

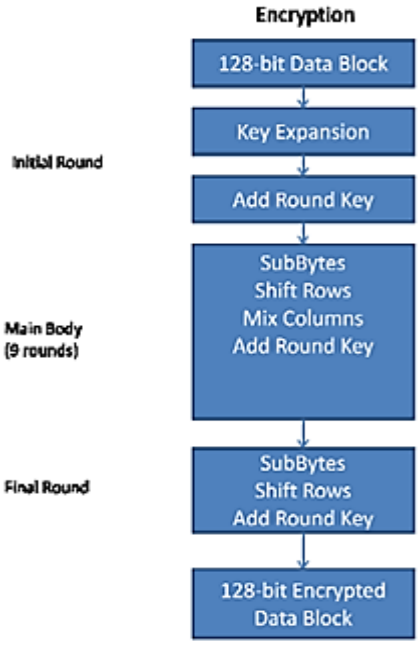


Fig. 2. Process of AES

- The data block is processed as follows:
- The AES Steganography routine begins by copying the 16-byte input array into a 4×4 byte matrix named State.
- Input Image block also known as state is XOR ed with the first 128-bits of the cipher key.
- Then the resulting State is serially passed through 10/12/14 rounds.
- The result of the last round is Watermarked image.
- The process of AES Steganography algorithm using 128-bit key, is diagrammatically represented in figure 2.

Functions of Advanced Encryption Standard:

- Sub Bytes()
- Shift Row()
- MixColoum()
- Add Round Key()

Direction Cosine Transform (DCT):

The direction cosine transforms (DCT) it has a sturdy toughness and is widely used in digital watermarking process. It is a time domain signal into its incidence components. The incidence coefficient is from DCT, such as single direct current, low frequency, mid frequency coefficient and high frequency coefficients. These middle frequency bands chosen that they avoid most visual part without over-exposing themselves to removal through compression and noise attacks [9].

Proposed Algorithm for the process:

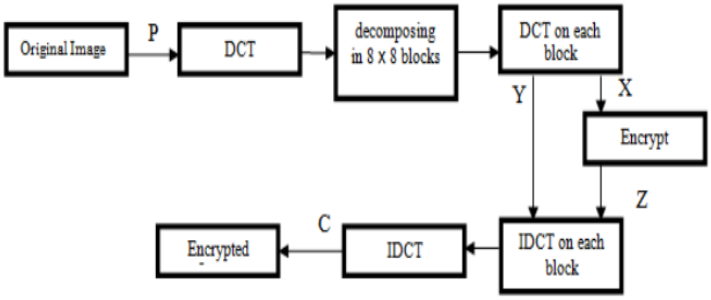


Figure 4. Block diagram of the proposed method

In the proposed system the Advanced Encryption Standard (AES) is an Steganography algorithm for securing sensitive data. It has been adopted by the United States government as an Advanced Steganography Standard, a standard algorithm used to Watermark and decrypt sensitive information. AES is a symmetric block cipher with a block size of 128 bits. It allows for three different key lengths which can be 128 bits, 192 bits, or 256 bits; referred to as AES- 128, AES-192, and AES-256, respectively. The number of rounds in the Steganography process for AES-128 is 10, for AES-192 it is 12, and for AES-256 it is 14.

III. RESULTS AND DISCUSSION

ADVANTAGE OF PROPOSED SYSTEM

The advantage of the proposed system of the steganography is

- More Bit per pixel ratio
- High Compression ratio
- Complex free computation

Hiding technique for embedding process:

It takes a cover video and a secret message as the input to the technique for hiding the data

Step 1: First take an original video as cover video. Then convert it into number of frames or images. Then select a particular frame/image; this will act as cover image.
Step 2: Add a password graphically for more security.
Step 3: Load a secret text which embed into the cover image and convert it into binary form.
Step 4: Then apply the AES technique. The AES bit of the video frame is replaced by the binary data. Then get a stego video
Step 5: Apply the combined DCT technique to stego-video.
Step 6: At last, encrypt the data and IDCT is applied to each block and the data is encrypted and the text is viewed.

SYSTEM REQUIREMENTS

The purpose of system requirement specification is to produce the specification analysis of the task and also to establish complete information about the requirement, behavior and other constraints such as functional performance and so on. The goal of system requirement specification is to completely specify the technical requirements for the product in a concise and unambiguous manner.

HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net
- Tool : Visual Studio 2010

IV.CONCLUSION

In this paper, we design a secure reversible image data hiding (RIDH) scheme operated over the encrypted domain. We suggest a public key modulation mechanism, which allows us to embed the data via simple XOR operations, without the need of accessing the secret encryption key. At the decoder side, we propose to use a powerful two-class SVM classifier to discriminate encrypted and non-encrypted image patches, enabling us to jointly decode the embedded message and the original image signal perfectly. We also have performed extensive experiments to validate the superior embedding performance of our proposed RIDH method over encrypted domain.

V. REFERENCES

[1]. M. U. Celik, G. Sharma, A. Tekalp, and E. Saber,"Lossless generalized-lsb data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp.253-266, 2005

[2]. M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless watermarking for image authentication: a new framework and an implementation," IEEE Trans. Image Process., vol. 15, no. 4, pp. 1042-1049, 2006.

[3]. Z. Ni, Y. Shi, N. Ansari, and W. Su,"Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, 2006.

[4]. X. Li, W. Zhang, X. Gui, and B. Yang,"A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," IEEE Trans. Inf. Forensics Secur, vol. 8, no. 7, pp. 1091-1100, 2013.

[5]. C. Qin, C.-C. Chang, Y.-H. Huang and L.-T. Liao,"An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109-1118, 2013.

[6]. W. L. Tai, C. M. Yeh, and C. C. Chang,"Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906-910, 2009.

[7]. J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, 2003.

[8]. Y. Hu, H. K. Lee, and J. Li, "De-based reversible data hiding with improved overflow location map," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 2, pp. 250-260, 2009.

[9]. X. Li, B. Yang, and T. Zeng,"Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524-3533, 2011.

[10]. X. Zhang,"Reversible data hiding with optimal value transfer," IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316-325, 2013.

[11]. T. Bianchi, A. Piva, and M. Barni,"On the implementation of the discrete fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Secur., vol. 4, no. 1, pp. 86-97, 2009.

[12]. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Secur., vol. 5, no. 1, pp. 180-187, 2010.

[13]. M. Barni, F. P., R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-preserving ecg classification with branching programs and neural net-works," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 2, pp. 452-468, 2011.

[14]. Z. Erkin, T. Veugen, T. Toft, and R. Lagendijk,"Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 3, pp. 1053-1066, 2012.

[15]. M. Chandramouli, R. Iorga and S. Chokhani, "Cryptographic key man-agement issues and challenges in cloud services," NIST Report 7956, pp. 1-31, 2013