Eleyon
SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY
Full Length Article

Secured Transmission of Medical Data using Encryption and Video Watermarking

K.Mohanapriya, P.Ananthi , J.Aysha Fathima Afreena , K.Guhan

[a]*Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode-638012, Tamilnadu, India*
[a]*Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode-638012, Tamilnadu, India*
[a]*Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode-638012, Tamilnadu, India*
[a]*Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode-638012, Tamilnadu, India*

***Corresponding Author**
afreenajahir@gmail.com
(J.Aysha Fathima Afreena)
Tel.: +91 8870355638

Received : 19-7-2017
Reviewed : 25-7-2017
Revised : 26-7-2017
Accepted : 05-8-2017

DOI:

ABSTRACT: The interrelated and highly sensitive issues of the medical image are security and privacy. Protecting the privacy and data integrity has to be done without comprising on the structural integrity of the data. The two layers of security are provided by watermarking and encryption. The watermarking is proposed to be implemented using a hybrid approach which encompasses Inter pulse code modulation and Singular Value Decomposition (SVD) techniques. Bit XOR Optimization is used for optimizing the watermarking parameters. The encryption is proposed to be effected using Data Encryption Standard (DES) and Transposition encryption algorithms. H.264 video codec is the most effective video compression standard developed in video industries. H.264 uses more accurate predication algorithms maintain the same quality video at a low bit rate, without compromising the image quality. A Graphical User Interface (GUI) which enables the user to have ease of operation in loading, watermarking, encrypting and also retrieving the original image whenever necessary is also designed. To check the robustness and the integrity of the watermark, different performance parameter

1 Introduction

The widespread use of the Internet and the World Wide Web has changed the way digital data is handled. The easy access of images and videos has changed the development of data hiding, by placing emphasis on content-based authentication, copyright protection, tamper proofing, annotation, and covert communication. Data hiding deals with the ability of embedding data into a digital cover with a minimum amount of perceivable degradation, i.e., the embedded data is invisible or inaudible to a human observer. The two sets of data in data hiding are cover medium and embedding data. The cover medium and the message can be text, audio, picture or video depending on the size of the message and the capacity of the cover. Data hiding and watermarking techniques are usually studied together because a watermarking technique can serve as a data hiding technique, as well, although the opposite is not always feasible. Early video data hiding approaches were essentially still imaged watermarking techniques extended to video by hiding the message in each frame independently. Transform domain is generally preferred for hiding data since, for the same robustness as for the spatial domain, the result is more pleasant to the Human Visual System (HVS). For this purpose the Discrete Fourier Transform (DFT), the Discrete Cosine Transform (DCT), and the Discrete Wavelet Transform (DWT) domains were usually employed. Recent video data hiding techniques are focused on the characteristics generated by video compressing standards. MPEG algorithms are used for motion vector based schemes. Video encoder calculates the motion vectors to remove the temporal redundancies between frames. Only a few data hiding algorithms considering the properties of H.264 standard have recently appeared in the open literature.

2 Proposed Methods

In this paper, encryption, and data embedding performance done on the compressed domain. A data hiding algorithm that works in the encrypted domain and preserves the confidentiality of the content. The proposed method for video encryption is to use standard stream cipher (RC4) with encryption keys. And after video encryption, codeword substitution technique generates pseudorandom sequence as data hiding key & embed the data into the encrypted video stream without knowing the original content. Data embedding done on the encryption domain gives poor image quality, data loss in the decrypted video.

2.1 Discrete Wavelet Transform (DWT)

Wavelets are the functions which are defined over a finite interval and have an average value equal to zero. The wavelet transform represents any arbitrary function (t) as a superposition of a set of the basis function. These basis functions called the baby wavelets are obtained from a single prototype wavelet called the mother wavelet. Basis functions include scaling function and wavelet function. The image is divided into different blocks and each block is then passed through the two filters, namely scaling filter (basically a low pass filter) and wavelet filter (basically a high pass filter). After the first level of decomposition four sub-images are formed namely LL, LH, HL, and HH coefficients.

At level 1: Image is decomposed into four subbands: LL, LH, HL, and HH where LL denotes the coarse level coefficient which is the low-frequency part of the image. HL, LH, and HH denote the finest scale wavelet coefficient. The LL subband can be decomposed d further to obtain a higher level of decomposition. This process of decomposition continues until the desired level of decomposition is achieved. The secure image can also be embedded in the remaining three sub-bands to maintain the quality of the image as the LL subband is more sensitive to the human eye. The discrete wavelet transform is a multi-resolution decomposition of a signal. The low pass filter applied along a certain direction extracts the low-frequency coefficients of a signal. The high pass filter extracts the high-frequency coefficients of a signal. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For next each successive level of decomposition, in our proposed approach the LH subband of the previous level is used as the input.

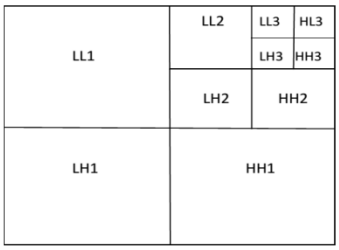

Fig. 1 *Three-level DWT decomposition*

2.2 Hybrid DWT-SVD Image Hiding Embedding Algorithm

The embedding algorithm for DWT-SVD based image hiding is shown in Fig.2, the algorithm works as follows,

Step 1: The cover N*N RGB image is transformed into sub-bands using single-level 2-D DWT.

Step 2: SVD is performed on LL sub-band of decomposed RGB cover image.

Step 3: The secret image (watermark) of size M*M RGB image is transformed into sub-bands using single-level 2-D DWT.

Step 4: SVD is performed on LL sub-band of decomposed RGB secret image.

Step 5: After performing SVD on both cover and secret images, the resultant image is then embedded with the cover image using the scale factor (α).

Step 6: The process of inverse SVD is performed on the embedded image.

Step 7: Finally, inverse 2-D DWT is performed to produce the resultant (watermarked) image.

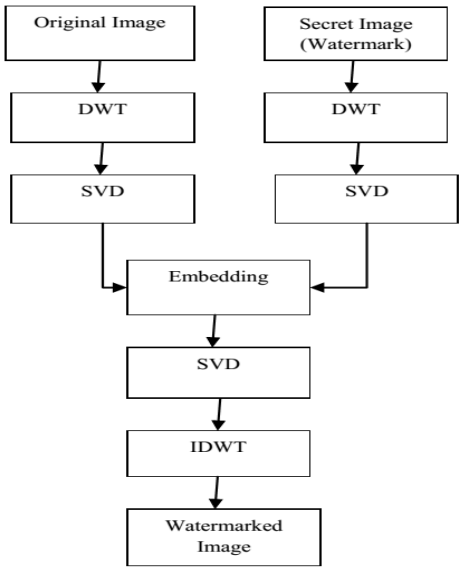

Fig.2 *DWT-SVD based Embedding*

2.3 Hybrid DWT-SVD Image Hiding Extraction Algorithm

The extraction algorithm for DWT-SVD based

image hiding is shown in Fig.3, the algorithm works as follows,

Step 1: The cover N*N RGB image is transformed into sub-bands using single-level 2-D DWT.

Step 2: SVD is performed on LL sub-band of decomposed RGB cover image.

Step 3: The secret image (watermark) of size M*M RGB image is transformed into sub-bands using single-level 2-D DWT.

Step 4: SVD is performed on LL sub-band of decomposed RGB secret image.

Step 5: The watermarked image is transformed into sub-bands using the single-level 2-D DWT.

Step 6: SVD is performed on LL sub-band of the decomposed RGB watermarked image.

Step 7: Using the same value of scale factor (α),

The extraction is applied to the SVD image.

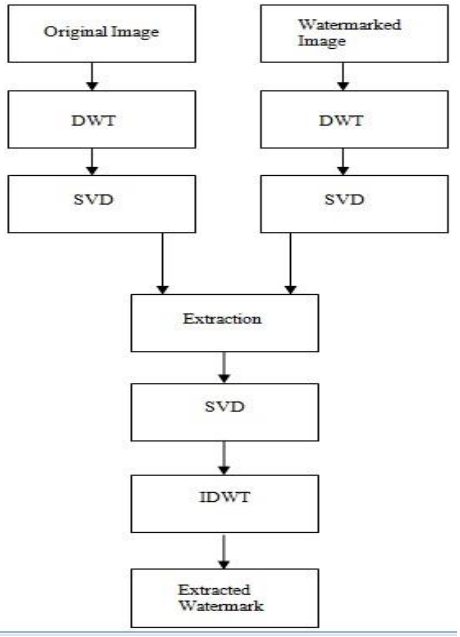

Fig. 3 *DWT-SVD based Extraction*

3 H.264 Prediction And Motion Estimation

Prediction is an important layer in video codec and playing an important role in compression and decompression. Prediction is used to remove spatial redundancy from the individual image and temporal redundancy from moving images. IPCM and interframe prediction are two types of prediction are used in video codec standards.

3.1 Inter Pulse Code Modulation

IPCM is one form of compression that looks at information of an individual frame and tries to reduce the amount of information with minimum loss and high quality. By doing intra prediction, spatial redundancy is removed from individual frame.H.264 is macroblock oriented and motion compensation based video codec standard. In H.264, a macroblock can be variable. macroblock size could be 16*16 and divided into the size of 16*8,8*16. Macroblock size could be 8*8 and divided into the size of 8*4,4*8 or merged into the size of 8*16 or 16*8. The 4*4 macroblock could not be divided into sub-blocks. a bigger macroblock covers a large area of the frame and more information. The higher macroblock size is used to code a continuous area of the picture. The smaller macroblock size is used to capture minor changes in frame with respect to another frame. In other words, higher macroblock size reduces the quality of the reconstructed image, but also decrease computation cost and complexity of the algorithm.A smaller macroblock is improved quality of the reconstructed image, but also increase computation cost and complexity of the algorithm. Impact of the macroblock is on compression is explained in figure 3.6. Figure 3.6 shows the variable size of the macroblocks.16*16 macroblocks. A 16*16 macroblock is divided into 16*8 or 8*16,16*8 or 8*16 block, it is encoded using two vectors. As we process 16*16 macro-block size with 4*4 macroblock size, a number of the encoded vector is sixteen. Thus, a selection of macro-block size is a trade-off between the precision in motion and the computational cost. An 8*8 macro-block size is considered for simulation in this project.

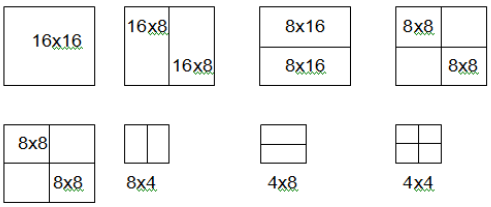

Fig.4 *H.264 macroblock size 16x16 ± 4x4*

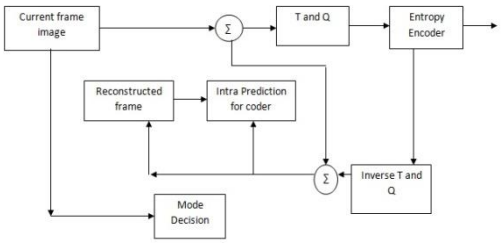

Fig.5 *Block diagram of Intraframe prediction*

Intraframe is divided into 8*8 macro-block size. The input of the mode selection block is the macro-block. The mode decision block selects one mode out of nine intra modes. A selection of intra mode is based on the sum of absolute error (SAE) or mean of absolute

difference (MAD) algorithms. SAD or MAD is calculated at mode selection points and the minimum result mode would be considered for only the current macro-block. The predictor macro-block is generated with respect to the reconstructed macro-block and the intra mode. The predicted macro-block is subtracted from the original macro-block and resulted as the residual macro-block. By discrete cosine transform and quantization, the residual macro-block is further processed. The output of quantization is applied to inverse quantization and inverse DCT and then generates the residual macro-block. The reference for next macro-block in the queue is the reconstructed residual macro-block. All nine modes are self-explained but we will discuss only mode-0 (vertical), mode-1 (horizontal) and mode-2 (DC). Fig.6 shows the direction of prediction in intra coding.

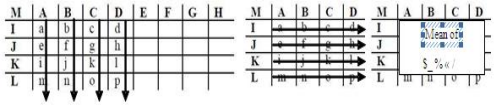

Fig.6 *The direction of prediction of intra mode mode-0,1,2 (left to right)*

3.2 Inter-Frame Prediction

Interframe prediction is also known as motion estimation or motion search. Frames can be predicted by single reference frame or multiple reference frames in inter-frame prediction. The direction of prediction can be one directional or bi-directional, which means a frame can be predicted considering previously coded frame or future frame or both. H.264 video codec standard improves performance because H.264 standard adds features such as accuracy as pixel level, multiple referencing and variable macro-block size as compared to previous standards. It is also applicable to interframe predictions. Considering Fig.6, each macro-block size is encoded with a single motion vector. Four motion vectors are needed for encoding 16x16 macro-block size with 8x8 sub-macro-block size. If we further divide an 8x8 macroblock into 4x4 sub-macro-block size, sixteen motion vectors are needed to encode 16x16 macro-block size with 4x4 sub-macro-block size. Thus, a macro-block is divided into multiple sub-macro-blocks to capture smaller motion in the image frame and needs a higher number of motion vectors to locate multiple sub-macro-blocks. Interframe prediction is the process of determining motions from one image to another. Motion vector defines displacement of a macro-block from one image with reference to another in terms of 2D coordinates of macro-block. Interframe prediction is the process of determining motions from one image to another. Motion vector defines displacement of a macro-block from one image with reference to another in terms of 2D coordinates of macro-block. Motion estimation creates a dummy current frame by modifying the reference frame such that the dummy current frame closely matches the original current frame. The objective of the motion search is to estimate the motion vector of the latest frame captured at time t with reference to another frame captured at time t.

3.3 Motion Estimation

Motion estimation searches for a motion vector of macro-block in the current frame with respect to a reference frame, and the searching motion vector is a heavy computation task in any video codec standards. In this project, three algorithms are studied in detail. The exhaustive search algorithm is one simple search algorithm. Three step search and four step search algorithms have less computational cost compared to full search algorithm with compromising image quality. The macro-block of the current frame is searched into the reference frame, and it is shown in Fig.7. This process is repeated until the perfect match is found in the reference frame. Fig.7 shows macro-block of the current frame (MB in light blue shade) is searched in the reference frame (I in yellow shade), within predefined search area (P in gray shade).

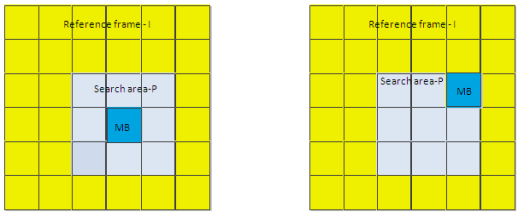

Fig.7 *Reference frame (I), search area (P), current macro-block (MB).*

A video has captured multiple image frames in a second. Those consecutive frames do not have much movement with respect to one another. The regular interval frame is chosen as a reference, and the following frames of the reference frame are known as a current frame. Reference frames have high movement and unacceptably high values of a cost function. In Fig.7, the reference frame and the current frame are shown with the size of MxM and are divided into an equal number of non-overlapped mxm macro-blocks. Each-macro-block of the current frame is compared with a limited number of macro-blocks in the reference frame as shown in the above figure. It is too costly to examine a macroblock of the current frame with all macro-blocks of the reference frame. MAD, SAD, and MSE are algorithms to get the best match. How much the macro-

block of the current frame is moved with respect to the reference frame is defined as the motion vector. This motion-vector will use by the motion compensation block.

3.4 Motion Compensation

Motion estimation and motion compensation techniques are employed to remove temporal redundancy between consecutive frames of the video data. After applying motion estimation the encoded frame has enough amount of temporal redundancy. The observation indicates that either a camera or an object is moving in the moving picture. The difference between consecutive frames of video data should result in motion of camera or motion of an object in frames. The results of motion estimation are motion vectors, but this output does not match with the desired output. The motion vector indicates the displacement of macro-block of the current frame in the reference frame. The H.264 has introduced a motion compensation block to remove complete temporal redundancy. Motion compensation regenerates a reference frame. The regenerated reference frame is more likely the current frame because the reference frame is generated using a motion vector of the current frame and a macro-block of the reference frame. The regenerated reference q frame is also known as a compensated frame. The difference between the current frame and the compensated frame is known as a residual frame.The residual frame contains only a camera motion or an object motion in the frame. Motion compensation transmits the predicted error, which has much less correlation with the original frame. The predicted error can be coded at a lower bit rate. The same prediction is generated at the receiver side and is combined with the received error to regenerate the current frame. Motion compensation enables low bit rates and low bandwidth features of H.264video codec. The motion compensation can be implemented by fixed block size, variable block size, overlapped block size, and half a pixel and quarter pixel. The current frame is divided into a number of non-overlapped macro-block. The motion vectors are extra information and require lots of memory on storage space. In fixed block size, the current frame is encoded as a conventional way. The variable block size utilizes block-matching compensation, with the ability to choose dynamic block size for the video encoder. Thus, VBMC(variable block motion compensation) requires a less number of bits to represent a motion vector by merging the macro-blocks into a large block.

4 Software Description

MATLAB® is a high-level language. It is an interactive environment for numerical visualization, computation, and programming. Using MATLAB, you can create models and applications, develop algorithms, analyze data. The tools, language, and built-in math functions help us to reach a solution faster than with spreadsheets or traditional programming languages, such as C/C++ or Java. MATLAB can be used for a range of applications, including image and video processing, control systems, signal processing, and communications, test and measurement, and computational biology. More than a million scientists and engineers in industry and academics use MATLAB for technical computing.

5 Output

5.1 Encryption

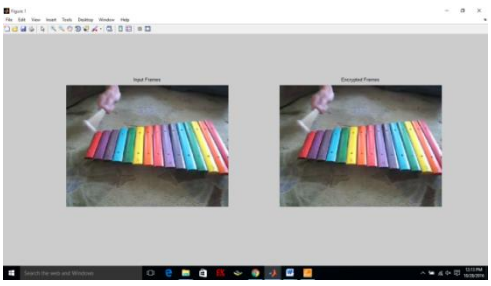

Fig.8.1 *Reading Video*

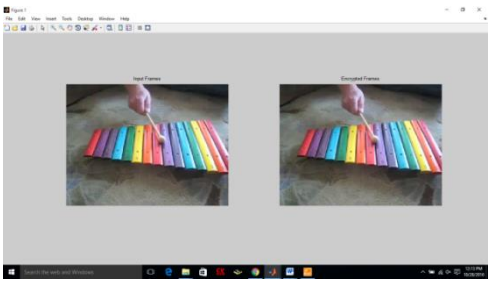

Fig.8.2 *Converting the video into frames*

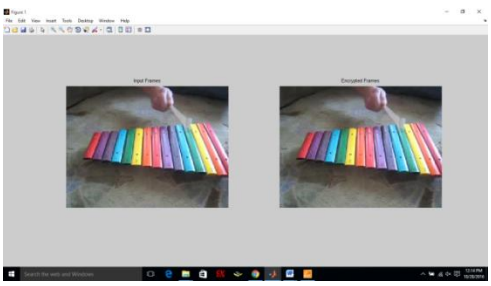

Fig.8.3 *Analysing the high motion frame*

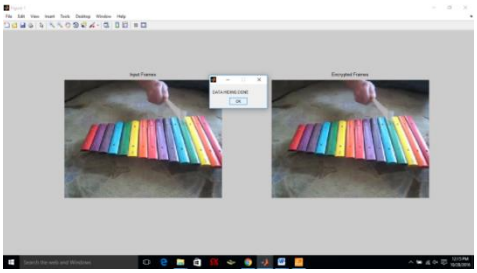

Fig.8.4 *Hiding data into frames*

5.2 Decryption

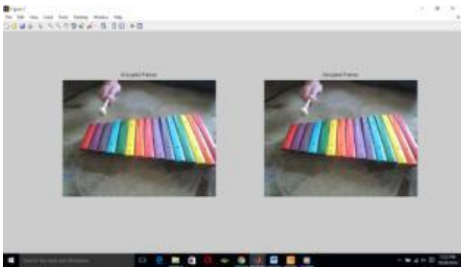

Fig.9.1 *Decrypting the frames*

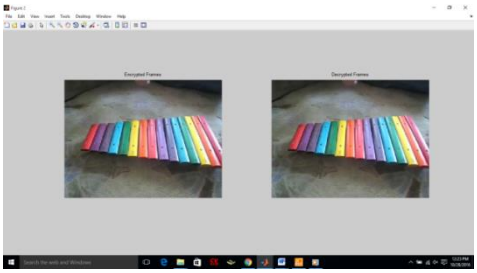

Fig.9.2 *Removing data from frames*

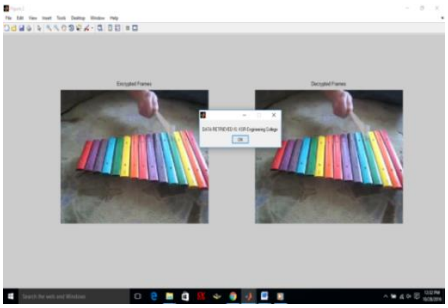

Fig.9.3 *Recovering the video after decryption*

6 Conclusion

H.264 video codec is the most effective video compression standard developed in Video industries. H.264 uses more accurate predication algorithms and motion compensation techniques to achieve better compression and same quality video at a low bit rate, without compromising the image quality. The H.264 encoder and decoder is implemented and simulated in the MATLAB and the simulation results give an idea about improvement made in H.264 standard. The focus of this project is motion estimation and motion compensation techniques. Motion estimation and motion compensation are the most computationally expensive and time-consuming process in the whole video compression process. The high definition video has very high temporal redundancy in the consecutive frames. This temporal redundancy can be removed with fast motion search algorithms and motion compensation. This process keeps only required information in the frames and forwards to other video compression blocks. The entropy coder outputs low bit rate information compared to the previously developed standards with the same video quality. A hybrid image-watermarking technique based on DWT and IPCM has been presented, where the watermark is embedded on the singular values of the cover image's three-level DWT LH3, HL3 sub-bands. The Experimental results of the proposed shown both the robustness under possible attacks. This paper proposed a novel technique for highly secure image data transmission using discrete wavelet transform (DWT) and Inter Pulse-code Modulation (IPCM) based image data hiding level. The technique ensures a higher efficiency of transmission security. This hybrid technique leads to optimize both the fundamentally conflicting requirements.

7 References

[1] An efficient wavelet-based watermarking algorithm Xiaojun Qi
[2] A Lossless Data-hiding Technique based On Wavelet Transform Hui-Yu Huang, Shih-Hsu Chang
[3] Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT) Nikita Kashyap
[4] Image Watermarking in DCT-DWT DomainAngshumi Sarma, Amrita Ganguly
[5] A Digital Watermarking Algorithm Based On DCT and DWT Mei Jiansheng, Li Sukang, Tan Xiaomei
[6] DWT Based Invisible Watermarking Technique for Digital Images Pallavi Patil, D.S. Bormane
[7] Digital Image Watermarking in Wavelet Domain H.E.Suryavanshi, Amit Mishra, Shiv Kumar
[8] Digital Image Watermarking in Wavelet Domain H. E. Suryavanshi, Amit Mishra, Shiv Kumar
[9] Digital Watermarking: Data Hiding Techniques using DCT-DWT Algorithm Kunal D Megha, Nimesh P Vaidya.