ISSN:2348-2079

Volume-5 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

An enhanced hybrid cryptographic and video watermarking for secure transmission of medical data

1. Mr. T.M.Saravanan, MCA., M.Phil.,
2. Ms. R.Kalaiselvi,
Department of Computer Applications-PG, Kongu Engineering College, Perundurai.
kalaikongu12@gmail.com

Abstract-- Medical image security and privacy are two issues that are interrelated and highly sensitive. Protecting the privacy and data integrity has to be done without comprising on the structural integrity of the data. Watermarking and encryption have served the purpose of data security for long. In this research work, a dual security approach is employed where watermarking and encryption is used to provide two layers of security. The watermarking is proposed to be implemented using a hybrid approach which encompasses Inter pulse code modulation and Singular Value Decomposition (SVD) techniques. BitXOR 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 same quality video at the low bit rate, without compromising the image quality. A Graphical User Interface (GUI) which enables the user to have ease of operation in loading the image, watermark it, encrypt it and also retrieve the original image whenever necessary is also designed. The robustness and the integrity of the watermark are tested by measuring different performance parameters and subjecting it to various attacks.

Keywords – Medical images; encryption; watermarking

I. INTRODUCTION

The widespread use of the Internet and World Wide Web has changed the way digital data is handled. The easy access of images, musical documents and movies has modified the development of data hiding, by placing emphasis on copyright protection, content-based authentication, 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.

Early video data hiding approaches were essentially still image watermarking techniques extended to video by hiding the message in each frame independently. Recent video data hiding techniques are focused on the characteristics generated by video com-pressing standards. Motion vector based schemes have been proposed for MPEG algorithms. Motion vectors are calculated by the video encoder in order to remove the temporal redundancies between frames. In these methods the original motion vector is replaced by another locally optimal motion vector to embed data. Only few data hiding algorithms considering the properties of H.264 standard have recently appeared in the open literature. In a subset of the 4 9 4 DCT coefficients are modified in order to achieve a robust watermarking algorithm for H.264. In the blind algorithm for copyright protection is based on the intra prediction mode of the H.264 video coding standard.

Traditionally, most of the data hiding techniques take place during the encoding either in the spatial or in the transform domain. Thus, for these techniques it is extremely difficult to perform data hiding in real time. Moreover, the access to the original video sequence is not always feasible and reuse of the marked video to hide different data is necessary. First decoding of the bit stream and then re-encoding it to embed the new data is needed. However, this results in video quality degradation, since the data hiding process has always some negative impact to the PSNR. Moreover, reusing the marked video, by decoding and re-encoding it, cannot always take place in real time. Other techniques, applied in the compressed domain, may

produce artifacts and drift errors, which degrade the video quality. Such errors make the reusing of the marked video in the compressed domain very ineffective. The proposed method addresses the aforementioned problems, i.e. data hiding in real time and reusing the marked video in real time without affecting video quality. In the recent few years, there is a serious problem about unauthorized and illegal access and manipulation of multimedia files over internet. Especially the case is more critical in the sense of image and video content privacy. Therefore a need for a robust method in order to protect the copy rights of media especially images and videos has become an essential constraint during the communication of secure images and videos over open communication channel. Invisible digital watermarking provides copyright protection of data by hiding the secure data inside a cover image or video. It is also done by embedding additional information called digital signature or watermark into the digital contents such that it can be detected, extracted later to make an assertion about the multimedia data. For image watermarking, the algorithms can be categorized into one of the two domains: spatial domain or transform domain [1,2]. In Spatial domain the data is embedded directly by modifying pixel values of the host or cover image, while transform domain schemes embed data by modifying transform domain coefficients [1,2]. Algorithms used for special domain are less robust for various attacks as the changes are made at Least Significant Substitution (LSB) of original data. While in the transform domain the watermark is embedded by changing the magnitude of coefficients in a transform domain with the help of discrete cosine transform, discrete interpulse code Modulation(IPCM) and singular value decomposition (SVD) techniques [3,5]. This provide most robust algorithm for many common attacks [7]. This paper proposed a novel technique for highly secure image data transmission based on discrete wavelet transform (IPCM) and Singular value decomposition (SVD) based image data hiding along with advance encryption standard (AES) to enhance the security level. Particularly IPCM and SVD based image data embedding over cover image is proposed to achieve higher robustness against various attacks, while AES ensures higher efficiency of transmission security. This hybrid technique leads to optimize both the fundamentally conflicting requirements. To present complete data security efficiency of the proposed technique various parameters like, peak signal to noise ratio (PSNR), mean square error (MSE), embedding rate (ER) and bit error rate (BER) have been employed.

II. LITERATURE REVIEW

A. A Joint Fed Watermarking Scheme

A joint FED watermarking system means joint finger print / encryption /dual watermarking system [1,6]. The system combines a region based substitution dual watermarking algorithm using spatial fusion, stream cipher algorithm using symmetric key, and fingerprint verification algorithm using invariants. Multiple document maintenance for a single patient such as digital X-ray image, personnel details, and diagnosis results are maintained and transmitted online separately which needs more time to process and gives poor quality image while decryption.

B. Encryption And Codeword Substitution Method

In this paper, encryption and data embedding performance done on the compressed domain. A data hiding algorithm that work entirely in the encrypted domain & thus preserves confidentiality of the content[4]. The proposed methodology 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. Dataembedding done on the encryption domain gives poor image quality, data loss in decrypted video.

III. PROPOSED ALGORITHM

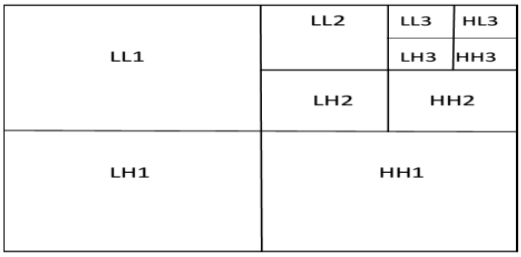
For ensuring the security and privacy of the information that is being communicated, a process called data encryption is essential. Encryption is carried out at the sending end. In this, sender transform the original information to another form, and sends the transformed information. At the receiving end, an exactly opposite process called Decryption is called out in which the received information is transformed back to its original form. Encryption and Decryption are carried out by the presentation layer.H.264 video codec is the most effective video compression standard

developed in video industries. H.264 uses more accurate predication algorithms maintain same quality video at the low bit rate, without compromising the image quality.

1. Interpulse code Modulation(IPCM)

IPCM are functions 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 basis function. These basis functions or baby wavelets are obtained from a single prototype wavelet called the mother wavelet. Basis functions include scaling function and wavelet function. The image is first divided into blocks and each block is then passed through the two filters: scaling filter (basically a low pass filter) and wavelet filter (basically a high pass filter). Four sub images are formed after doing the first level of decomposition namely LL, LH, HL, and HH coefficients[6-8].At level 1: Image is decomposed into four sub bands: LL, LH, HL, and HH where LL denotes the coarse level coefficient which is the low frequency part of the image. LH, HL, and HH denote the finest scale wavelet coefficient. The LL sub band can be decomposed further to obtain higher level of decomposition. This decomposition can continues until the desired level of decomposition is achieved for the application. The secure image can also be embedded in the remaining three sub bands to maintain the quality of image as the LL sub band is more sensitive to human eye.

Discrete wavelet transform is a multi-resolution decomposition of a signal. The low pass filter applied along a certain direction extracts the low frequency (approximation) coefficients of a signal. On the other hand, the high pass filter extracts the high frequency (detail) coefficients of a signal [7]. In 2D applications, for each level of decomposition, first perform the IPCM in the vertical direction, followed by the IPCM in the horizontal direction. 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 sub band of the previous level is used as the input. Each component undergoes three levels of decomposition. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band. The three-level IPCM decomposition is shown in Figure 1.



2. Singular Value Decomposition (SVD)

An image can be represented as a matrix of positive scalar values. The basic idea behind SVD technique of watermarking is to find SVD of image and the altering the singular value to embed the watermark. In Digital watermarking schemes, SVD is used due to its main properties: A small agitation added in the image, does not cause large variation in its singular values. The singular value represents intrinsic algebraic image properties [4].

Step By Procedure:

Step-1. Read video.

Step-2. Converting frames.

Step-3. Encryption frames using XOR.

Step-4. Frame divided into 4*4 or 8*8 or 16*16 block.

Step-5. Motion estimation based on inter intra frames using IPCM.

Step-6 . By using Data Encryption Standard(DES) technique encrypt the Secret data and then convert as interger values.

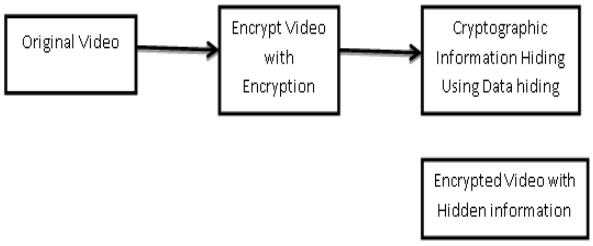
Step-7 . Find motion portion in frames for data embedding.

Step-8. After embedding frames converted into video.

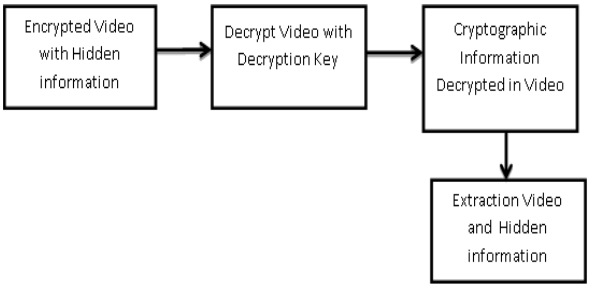
Step-9. Decrypt all frames from encrypted video.

Step-10 .Data retrive from decrypted frames.

For dewatermarking reverse process.



Overall Block Diagram: Encryption Section



Decryption Section

IV. SIMULATION RESULTS

The proposed algorithm was integrated within version JM14.0 of the reference H.264 software. The most important configuration parameters of the reference soft-ware are given in Table.1. The rest of the parameters have retained their default values. The IPCM, SVD macro blocks are expected to have a negative impact to the produced bit rate. We conducted several tests in order to investigate this impact. For that purpose we used 300 frames or 10 s of well-known representative video sequences in QCIF format (YUV 4:2:0) such as the akiyo (Class A), the foreman (Class B) and the mobile (Class C). The QCIF format (176 9 144) was chosen because it is very common in mobile applications where the demand for real time is always high. The three classes that we used for our experiments possess the following characteristics:

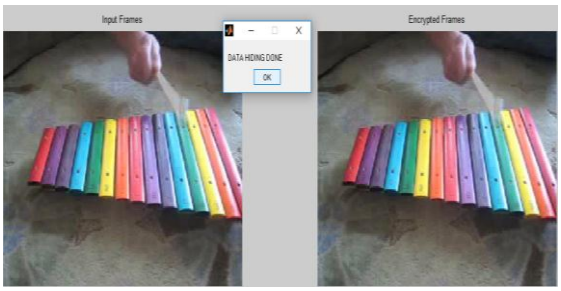
Class A: Low spatial detail and low amount of movement;

Class B: Medium spatial detail and low amount of movement or vice versa;

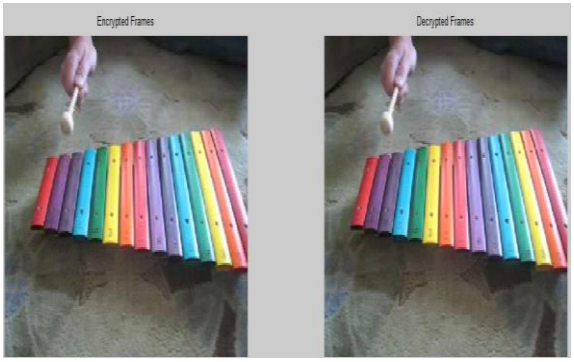
Class C: High spatial detail and medium amount of movement or vice versa. Table 1 Configuration parameters of the encoder.

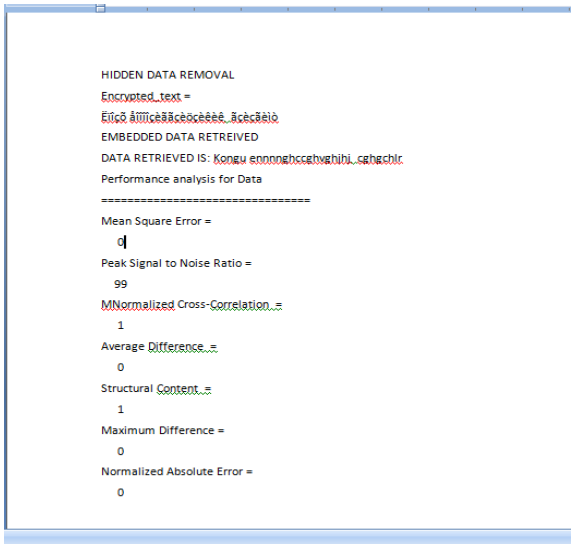
Profile	Main
Number of frames	300 (10 s)
Frame rate	30 fps
RD optimization	High complexity mode
Motion estimation	Simplified UMHexagonS
Intra period	0: only the first frame is intra
Symbol mode	CABAC

ENCRYPTION OUTPUT



DECRYPTION OUTPUT:PSNR Value=99 db





V. CONCLUSIONS

This paper proposed a novel technique for highly secure image data transmission using discrete Interpulse code Modulation (IPCM) and Singular value decomposition (SVD) based image data hiding level. Technique ensures higher efficiency of transmission security. This hybrid technique leads to optimize both the fundamentally conflicting requirements. To present complete data security efficiency of the proposed technique various parameters like, peak signal to noise ratio (PSNR), mean square error (MSE), embedding rate (ER) and bit error rate (BER) have been employed. A complete visual and subjective analysis have been included in this paper to present high image data embedding and extraction efficiency of proposed system. After successful implementation of proposed system in MATLAB 2014(b) software platform, the proposed system is tested for four test cover images with the variable scaling factor scenario.

REFERENCES

1. Bouslimi.D, Coatrieux.G and Roux.C, "A joint encryption watermarking system for verifying the reliability of medical images," *IEEE Trans. Inf.Technol. Biomed.,* vol. 16, no. 5, pp. 891-899, 2012.

2. Hong W, Chen W and Wu H, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

3. Liu W, Zeng W, Dong L and Yao Q, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp.1097–1102, Apr. 2010.

4. Spyridon K. Kapotas, Athanassios N. Skodras, "Real time data hiding by exploiting the IPCM, SVD macro blocks in H.264/AVC streams" , Springer Journal of Real Time Image Processing, Volume 1, Issue 4,March 2009.

5. Luo L, Chen Z, Chen M, Zeng X and Xiong Z, "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 1, pp. 187–193, 2010.

6. Wang S andYandsheng W, "Fingerprint enhancement in the singular point area,"*IEEETrans.Image Process.*, vol. 9, no.1, pp. 16-19, 2013.

7. Zhang X, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

8. Zhao B, Kou W.D and Li H, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," *Inf. Sci.*, vol. 180, no. 23, pp. 4672–4684, 2010.

9. Zheng P.H and Huang J.W, "Walsh-Hadamard transform in the homomorphic domain and its application in image watermarking," in *Proc. 14th Inf. Hiding Conf.*, Berkeley, CA, USA, pp. 1–15, 2012.