A New Technique for Protecting Confidential information Using Watermarking

Gayathri.M[1],Pushpalatha.R[1], Yuvaraja.T[2]

[1]PG Scholar, Department of ECE, kongunadu College of Engineering and Technology, Tamilnadu, India

[2]Assitant Professor, Department of ECE, kongunadu College of Engineering and Technology, Tamilnadu, India

E-mail- mgayathri01@gmail.com

ABSTRACT - A new approach of image watermarking based on RSA encryption technique for the lossless medical images has been proposed. This paper presents a strategy of attaining maximum embedding capacity in an image in a way that to determine the amount of information to be added in each pixel, maximum possible neighboring pixels are analyzed for their frequencies. The technique provides a seamless insertion of image into carrier video, and reduces the error assessment and artifacts insertion required to a minimal. Two or more bits in each pixel can be used to embed message, which has high risk of delectability and image degradation to increase the embedding capacity. The RSA techniques might use a significant bit insertion scheme, the bits of data added in each pixel remains constant or a variable least significant bit insertion in which the number of bits added in each pixel vary on the surrounding pixels to avoid degrading the image fidelity.

Keywords: watermarking, mean square error, encryption, decryption, SPHIT, wavelet, RSA algorithm.

1. INTRODUCTION

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light, caused by density variations or thickness in the paper. Watermarks have been used have been on currency, postage stamps, , and other government documents to discourage counterfeiting. Watermarks are often used as security features of passports, banknotes, postage stamps, and other documents to prevent counterfeiting. Encoding an identifying code into digitized video, music, picture, or other file is known as a digital watermark.

A watermark is made by impressing a water-coated metal stamp or dandy roll onto the paper during manufacturing. Artists can copyright their work by hiding their name within the image. It is also applicable to other media, such as digital video and audio. There are a number of possible applications for digital watermarking technologies and this number is increasing rapidly. For example, in data security, watermarks may be used for authentication, certification, and conditional access. Certification is a vital issue for official documents, like identity cards or passports.

2. RSA Algorithm

RSA is associate algorithmic program for public-key cryptography that's supported the probable problem of factorization large integers, the factorization drawback. A user of RSA creates and so publishes the product of two large prime numbers, in conjunction with an auxiliary value, as their public key. The prime factors should be unbroken secret. Anyone will use the general public key to encrypt a message, however with presently published methods, if the general public key is large enough, only someone with information of the prime factors will feasibly rewrite the message. whether or not breaking RSA secret writing is as hard as factoring is associate open question referred to as the RSA drawback.

The RSA algorithmic program involves 3 steps, it is given below

- Key generation
- Encryption
- Decryption

2.1 Key generation

RSA involves a public key and a non-public key(private key). The general public key is well-known by everybody and is employed for encrypting messages.

Messages encrypted with the general public key will solely be decrypted in a very affordable quantity of your time using the non-public key.

2.2 Encryption

For example, Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then desires to send message M to Alice.

He initial turns M into a whole number m, such 0 ≤ m < n by exploitation an agreed-upon reversible protocol referred to as a padding scheme. He then computes the cipher text c like

$$c \equiv m^e \pmod{n}.$$

2.3 Decryption

Alice will recover m from c by exploitation her non-public key (private key) exponent d via computing

$$m \equiv c^d \pmod{n}.$$

Given m, she will be able to recover the original message M by reversing the artifact theme

3. DISCRETE WAVELET TRANSFORM

It permits the image decomposition in several styles of coefficients conserving the image information. Such coefficients coming from completely different images are suitably combined to get new coefficients in order that the data within the original images is collected befittingly. In discrete wavelet transform (DWT), two channel filter bank is employed. When decomposition is performed, the approximation and detail element is separated 2-D discrete wavelet Transformation (DWT) converts the image from the spatial domain to frequency domain.

4. PEAK SIGNAL TO NOISE RATIO

PSNR is most typically used to measure the standard of reconstruction of loss compression codec's (e.g., for image compression). The signal during this case is that the original information, and therefore the noise is that the error introduced by compression. Once examination compression codec's, PSNR is approximation to human perception of reconstruction quality. Although the next PSNR typically indicates that the reconstruction is of upper quality, in some cases it's going to not.

PSNR is most simply outlined via the mean square error (MSE).

Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is outlined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$PSNR = 20.\log_{10}(MAX\ I) - 10.\log_{10} MSE$$

Here, MAX_I is that the most attainable pixel value of the image. when the pixels are delineated mistreatment eight bits per sample, this can be 255.

For color pictures with three RGB values per images, the definition of PSNR is that the same except the MSE is that the total over all squared value variations divided by image size and by three. Alternately, for color pictures the image is regenerate to a unique color space and PSNR is reported against every channel of that color space.

4.1 Testing Topology

Depending on the knowledge that's created obtainable to the algorithmic rule, video quality check algorithms may be divided into 3 categories:

1. A "Full Reference" (FR) algorithm has access to and makes use of the original reference sequence for a comparison (i.e. a difference analysis). It can compare each pixel of the reference sequence to each corresponding pixel of the degraded sequence. FR measurements give the highest accuracy and repeatability but tend to be processing intensive.

2. A "Reduced Reference" (RR) algorithm uses a reduced side channel between the sender and the receiver which is not capable of transmitting the complete reference signal. Instead of parameters are extracted at the causation aspect that helps predicting the standard at the receiving side. RR measurements might supply reduced accuracy and represent a working compromise if information measure for the reference signal is restricted.

3. A "No Reference" (NR) algorithm only uses the degraded signal for the quality estimation and has no information of the original reference sequence. NR algorithms are low accuracy, estimates only as the originating quality of the source reference is completely unknown. A common variant of NR algorithms does not analyze the decoded video on a pixel level but work on an analysis of the digital bit stream on an IP packet level, only. The measurement is consequently restricted to a transport stream analysis.

Peak Signal to Noise magnitude relation (PSNR) could be a ubiquitously used image process performs to compare two pictures. It the foremost rudimentary estimate on the distinction between two pictures and is predicated on mean square error (MSE).

5. BLOCK DIAGRAM

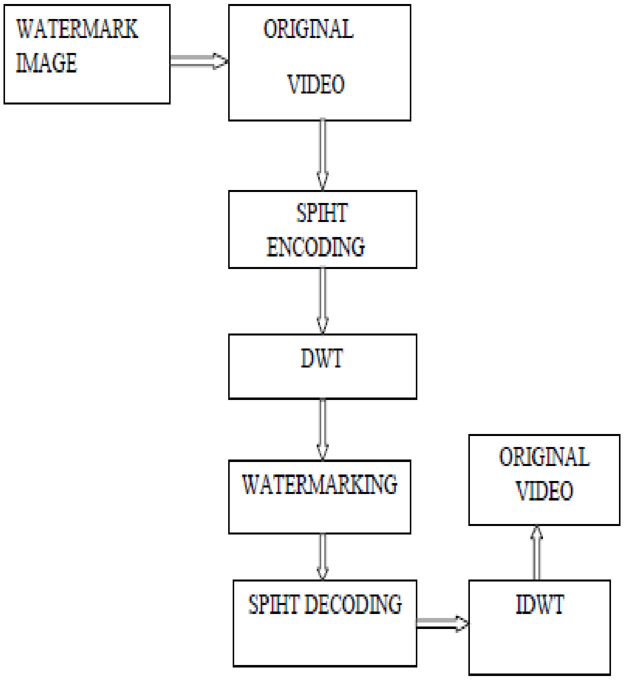

Fig-1 Block diagram of the System

To hide an image into the carrier video, the image is encoded using SPIHT and then apply the discrete wavelet transform. Watermarking is used to hide that image into video. After hide tha image into the video. There is no difference between the input video and the watermarking video. The image can be recovered by using the SPIHT decoding and inverse wavelet transform.

The output is given below

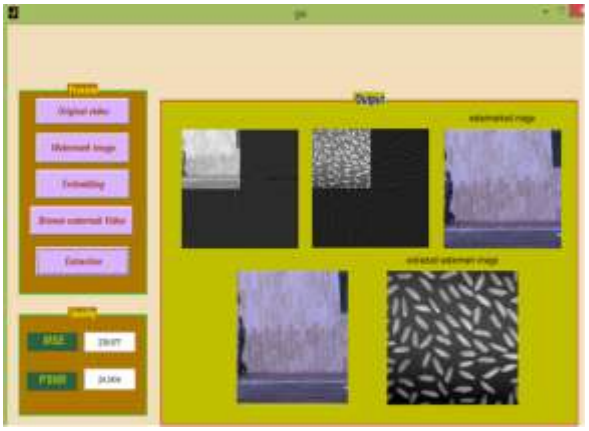

Fig-2 output

6. CONCLUSION

The watermarking is used in the covert communication to transport secrete information. if to hide the secret message into an image means the secret message is embedded into smaller matrix of size 8x8 and inserted into input image. In this paper the RSA algorithm process is used to hide an image into the video. Video is used as a carrier. The improvement of this application would be extending its functionality to support hiding data in video files or in other file format.

REFERENCES:

[1] Ayman Ibaida, Ibrahim Khalil(2013), ‘Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems’ IEEE Transactions on Biomedical Engineering,pp.1-9.

[2] Golpira. H and Danyali. H(2009), ‘Reversible blind watermarking for medical images based on wavelet histogram shifting, IEEE,pp. 31–36.

[3] Ibaida. A, Khalil. I, and Sufi. F(2010), ‘Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis(PCA),’ pp.207–212.

[4] Kaur. S, Singhal. R, Farooq. O, and Ahuja. B(2010), ‘Digital Watermarking of ECG Data for Secure Wireless Commuication’, pp. 140–144.

[5] Lee .W and Lee C.(2001), ‘A cryptographic key management solution for hipaa privacy/security regulations’, vol. 12, no. 1.,pp. 34-41.

[6] Malasri. K and Wang. L (2007), ‘Addressing security in medical sensor networks’, ACM, p. 12.

[7] Marvel. L, Boncelet. C, and Retter. C.(1999), ‘Spread spectrum image steganography’, vol. 8, no.8, pp. 1075–1083.

[8] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou(2013), ‘Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption’ vol. 24, no. 1., , pp. 131-143.

[9] Wang. H, Peng. D, Wang .W, Sharif. H, Chen. H, and Khoynezhad. A(2010), ‘Resource-Aware secure ECG healthcare monitoring through body sensor’ vol.17, no.1., pp. 12-19,.

[10] Zheng. K and Qian. X (2008), ‘Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transform’ CIS’08, vol. 1,.

[11] Fei Hu, Meng Jiang(2007), ‘Privacy-Preserving Telecardiology Sensor Networks:Toward a Low-Cost Portable Wireless Hardware/Software Codesign’ vol.11,no.6.

[12] Y. Lin, I. Jan, P. Ko, Y. Chen, J. Wong(2004), “A wireless PDA-based physiological monitoringsystem for patient transport”, vol. 8, no. 4,pp. 439–447,.