Authentication Medical Data and Image for Steganography and Watermarking Technique

Ms. Payal Gupta[1], Prof. (Dr.) Sudhir Kumar Sharma[2], Mr. Harsh Shrivastava[3]

P. hd. Scholar, Department of Electronics and Communication Engineering, Jaipur National University, Jaipur Rajasthan[1]
Head of Department, Department of Electronics and Communication Engineering, Jaipur National University, Jaipur, Rajasthan[2]
Assistant Professor, Department of Electrical Engineering, Jaipur National University, Jaipur, Rajasthan[3]

Abstract— Nowadays, the success of internet technology, made our life very much easy and convenient. But the major problem is to secure the data from duplication and unauthorized use. So the digital watermarking is used. With this technology, we embed the secret information into the actual information for protecting it from unauthorized use. By using this technique only authorized user can access the data. The available methods till data result in good PSNR but they are not secure image.
"Steganography" is a technique that thwarts unauthorized users to have access to the crucial data, to invisibility and payload capacity using the different technique like discrete cosine transform (DCT) and discrete wavelet transform (DWT).The available methods till date result in good robustness but they are not independent of file format.
The aim of this research work is to develop independent of file format and secure hiding data scheme. Accordingly an efficient scheme is developed with the combine watermarking and steganography technique.

Keywords— Discrete Wavelet Transform, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE)

I. INTRODUCTION

Now a day, most of the information in Computer processing is handled online. This online information is either graphical or pictorial in nature, and the storage and communication requirements are immense. Hence method of compressing the data prior to storage and transmission are of significant practical and commercial interest. Image compression means reducing the redundant amount of data required to represent a digital image. The Digital image compression in mathematical form can be defined as transformation of a 2-D pixel array by image, into a statistically uncorrelated data set. The transformation is applied on image prior to storage and transmission of Digital Image Data. The compressed image is reconstructed into original image by the process of Decompression. Decompressed image can be an original image or approximation of it. Image compression is the technology for handling the increased spatial resolutions of today's imaging sensors and evolving broadcast television standards. Image compression plays an important role in many important and diverse applications including tele video conferencing, remote sensing, document and medical imaging, facsimile transmission and the control of remotely piloted vehicles in military, space, and hazardous waste management applications. The application list is ever expanding on the efficient manipulation storage and transmission of different types of digital image such as binary images, gray-scale images, and color images etc. [1], [2] The Internet, still in its childhood; continues to flourish and impact on our personal and professional lives. Common to these and many other applications is the requirement of huge storage space and communication bandwidth for digital images. Hence digital media is motivated by innovative methods for compression of digital images for efficient utilization of storage space and communication bandwidth [3], [4]. In general context, the image speaking compression techniques can be divided into two broad classes: lossless compression and lossy compression schemes. Lossless Compression (Information preserving): As the name implies, this technique involves no loss of data. The original data can be recovered exactly from the compressed data.

A CT scan are on kind of special x-ray tests which is produce cross-sectional images of the body using computer and x-rays it plugs a major role in diagnosing medical diseases, it is used to know details of human body like chest, belly, pelvis, arm, leg, by using CT scan pictures of organ like liver, pancreas, intestine, kidney, bladder, adrenal gland, lung and heart, and etc. The MRI is a techniques to get a clear picture of organs by using large amount of magnetic and radio waves. It uses to diagnose a variety of conditions from ligaments to tumors and will be used to study brain and spinal cord. In medical image processing De-noising of images plays an important role to obtain precise and accurate images for further diagnosis. Medical images are collected by different sensors and they are also subjected wide variety of distortion, storage, compression, acquisition, processing, reproduction And transmission which causes them to get contaminated by different types of noises are removed using filters as they can produce best results depending upon its parameters. The selection of filters depend upon they type of noise because different type of noise can be removed using different types of noises. In this paper a noised image is considered and it is filtered using Median and Wiener filter and the result is compared on various parameters. Median filter and Wiener filter algorithm will be modified. Various noises and like salt and pepper noise are added. Wiener filter and median filter are implemented to remove additive noise which is present in MRI and CT scans which also responsible to add density gradually. Superconductive scanner contains refrigeration system and liquid helium pump which is responsible for "thump thump" sound, which is also irritate patient and leads temporary earring loss.

Data security is the most essential resource since loss of data will prompt numerous issues in electronic world. The three systems to be specific cryptography, steganography and watermarking structure the base for secure correspondences. Cryptography is a strategy in which the mystery message is scrambled and sent in an indiscernible arrangement. It scrambles the secret information such that it gives off an impression of being waste to any unapproved client. The mystery information to be imparted is a mix of stages and substitutions and consequently ill-conceived clients couldn't get to the message.

Steganography is a specialty of concealing the mystery data inside some other record for the most part known as the cover. The cover medium is picked deliberately so it mirrors some non-suspicious type of correspondence.

Figure 1: General schematic description of steganography with different types of covers

The primary target of steganography is to give an undercover correspondence between any two clients with the end goal that a unintended client does not access the data by simply observing the cover document. Steganography is not quite the same as cryptography. The fundamental contrast is that the last scrambles the information while the previous just conceals its essence. At the end of the day steganography conceals the information while cryptography scrambles the information. Steganography gives significantly more security when contrasted with cryptography in light of the fact that there is zero chance of any unintended client to realize that a message is being sent though in cryptography, there will dependably be a doubt that a mystery message is being sent. Consequently these are more inclined to be hacked.

Watermarking is for the most part utilized for validation and copyrights security. It can be utilized for making a picture with the goal that it is conspicuous. It can likewise be utilized to check an advanced document with the goal that it is proposed to be noticeable (obvious watermarking) or unmistakable just to its maker (imperceptible stamping). The principle target of watermarking is to maintain a strategic distance from the illicit duplicating or claim of responsibility for media. Cryptography and steganography could be utilized on private correspondence; typically for shared premise, however watermarking is utilized between one to numerous i.e. same watermark is implanted in numerous spreads. Fingerprinting is an uncommon sort of watermarking, which would install mark and serial number to recognize a one of a kind duplicate among a few.

II. DIGITAL WATERMARKING FEATURES

Joining profoundly metadata in sight and sound substance, advanced water checking systems is valuable despite the fact that, aside from accessibility of substitute components like header of a computerized record which stores meta-data. But since of following highlights the advanced watermarking system is engaging for the addition of unmistakable checks in video and pictures which additionally includes data about sound in sound clasp and so on [2].

Imperceptibility

The commendations of media are of the feeling that watermarks couldn't be modified as installed watermarks are committed without error and they are factually. Noticeable relics in still pictures are not made by watermarks. The watermarks don't adjust the bit rate of video or does not permit any capable of being heard frequencies in sound signs.

Robustness

The utilization of computerized watermarking is by and large for distinguishing proof of possession, so it isn't subjected for any change. The methods of advanced watermarking is fit for supporting distinctive levels of durability against changes assuming any, that can be made to the substance of watermark unconcerned application. The advanced watermarks debased or be demolished because of getting undesirable and hurtful signs and geometric contortions like symmetrical computerized transformation, computerized to simple change, editing, turn, disease, scaling, dithering, a pressure and so on of the substance. Then again in the event that it utilized for the confirmation of the substance. Those ought to effectively break or pulverized at whatever point, the substance is altered for the reason of adjusting the substance which is identified.

Inseparability

It isn't conceivable either to particular or get again into the first position of the watermark after implant with watermark is finished.

Security

Individuals, who are not unapproved, are not permitted to identify and change the watermarks which have been settled immovably in the cover motion by the advanced watermarking method and the keys of watermark guarantee that to distinguish and adjust watermark just approved people are allowed.

III. STEGANOGRAPHY

Steganography is in practice since ancient time for concealing the existence of a message inside another media. In a modern approach, the concept of contemporary steganography is explained in Figure 2. The secret message, which is to be transmitted, is embedded inside a cover file at sender premise. Digital image, text document, audio file, video file, etc. can be used as a cover file. A key might be related to the concealing procedure. The file obtained as a result of embedding message in a cover file is named as stego file which is communicated to the receiver. A similar method is followed at the receiver site, in reverse order, to extract the hidden message. Key plays the role of controlling parameter for hiding as well as extraction of the message at both the ends. Thus it is crucial for secure communication to make an intelligent choice regarding key selection.

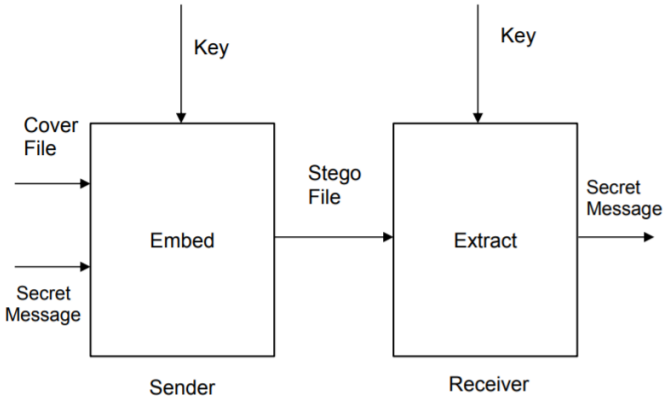

Figure 2: Steganography (Anderson, 1996)

The aforementioned discussion clarifies the goals of steganography. The prime goals of steganography itself act as an inspiration for a researcher to work in this area. It is worth

to mention at this point that out of the abovestated objectives; it becomes a tradeoff to achieve some of the goals while maintaining others at a satisfactory level.

IV. MRI IMAGE

MRIs employ powerful magnets which produce a strong magnetic field that forces protons in the body to align with that field. At the point when a radiofrequency current is then beat through the patient, the protons are animated, and turn out of balance, stressing against the draw of the attractive field.

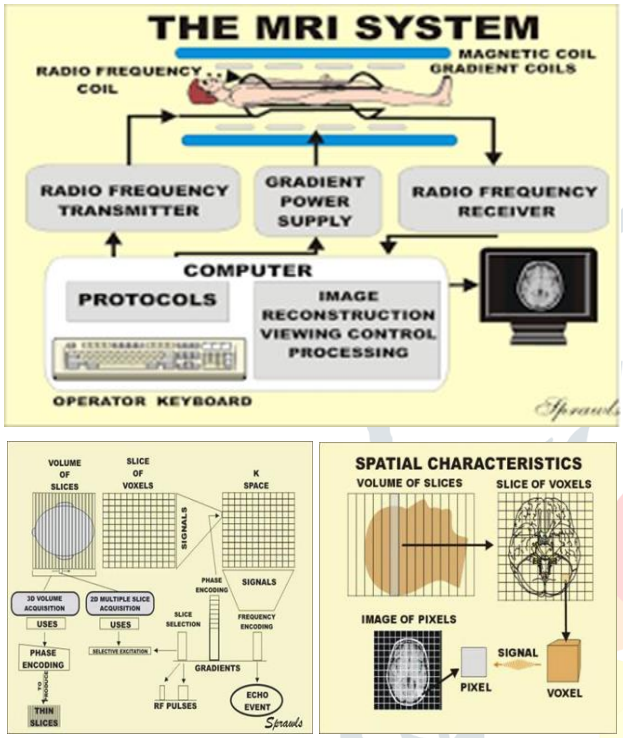

Figure 3: Working of MRI Image

At the point when the radiofrequency field is killed, the MRI sensors can identify the vitality discharged as the protons realign with the attractive field.

Attractive polarization .Very solid uniform magnet excitation .Very capable rf transmitter Acquisition, Location is encoded by angle attractive fields .Very effective audi amps Polarization, Proton have an attractive minute proton have turns like pivoting magnets Body has a great deal of protons.

V. PROPOSED METHODOLOGY

Watermarking Embedding procedure:

The procedure for embedding the watermark that we are following in this project is given as follows:

a. Select the host and the watermark image.

b. Apply DWT transform on both original and the watermark image.

c. Apply SVD on the LL sub band of both original and the watermark image.

d. Apply the watermarking algorithm on the two images and generate the resulting watermarked image.

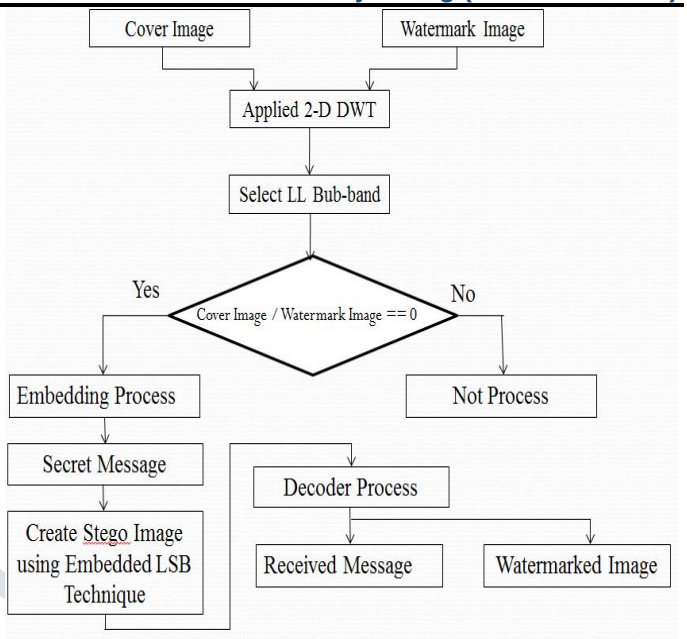

Figure 3: Flow Chart of Proposed Methodology

Algorithm

Step 1: Input Host image, Take cover image (CI).

Step 2: Apply 2-D DWT on CI to decompose it into four subbands.

Step 3: Select sub-band LL2 of CI.

Step 4: Take watermark image (WI)

Step 5: Apply 2-D DWT on WI to decompose into four subbands.

Step 6: Select sub-band LL2 of WI.

Step 7: Embedding Process

Step 8: Enter Secrete Massage

Step 9: Applied LSB technique for Encoder

Step 10: Find Stego Image

Step 11: Applied Decoder Process

Step 12: Finally get secrete message and watermarked image

VI. CONCLUSION

The cover images that are preprocessed are decomposed into Vertical, Horizontal and Diagonal components using Discrete Wavelet Transform. The sub band which has lowest noise density is taken and it is further decomposed. This process is continued up to various levels such that noise density is equal for all sub bands. The information to hide is encoded using encryption methods. The encoded sample values are embedded directly into the sub bands which are having low noise density.

Particular attention is given to the proposed scheme to guarantee secure watermark embedding and easy extraction. The new techniques could offer significant advantages to the digital watermark field and provide additional benefits to the copyright protection industry.

REFRENCES

[1] Wenguang He, Zhanchuan Cai and Yaomin Wang, "High-fidelity Reversible Image Watermarking Based on Effective Prediction Error-Pairs Modification", IEEE Transactions on Multimedia, IEEE 2020.

[2] A. Bose and S. P. Maity, ''Spread spectrum image watermark detection on degraded compressed sensing measurements with distortion minimization,'' Multimedia Tools Appl., vol. 77, no. 16, pp. 20783–20808, Aug. 2018.

[3] Awdhesh K. Shukla, Akanksha Singh, Balvinder Singh and Amod Kumar, "A Secure and High-Capacity Data-Hiding Method using Compression, Encryption and Optimized Pixel Value Differencing", IEEE Access, October 8, 2018.

[4] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption", Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

[5] Baharak Ahmaderaghi ; Fatih Kurugollu ; Jesus Martinez Del Rincon ; Ahmed Bouridane, "Blind Image Watermark Detection Algorithm based on Discrete Shearlet Transform Using Statistical Decision Theory", IEEE Transactions on Computational Imaging, Volume: 4 , Issue: 1, Page s: 46 – 59, IEEE 2018.

[6] S. P. Maity and S. Maity, ''On detection improvement in MC-CDMA image watermarking on fading channel,'' Wireless Pers. Commun., vol. 100, no. 2, pp. 587–609, May 2018.

[7] X. Xie, Z. Xu, and H. Xie, ''Channel capacity analysis of spread spectrum watermarking in radio frequency signals,'' IEEE Access, vol. 5, pp. 14749–14756, Oct. 2017.

[8] Q. Zhou, G. Zang, and H. Song, ''DSSS signal detection method based on cyclic Spectrum,'' Commun. Technol., vol. 50, no. 11, pp. 2419–2425, Nov. 2017.

[9] H. Xing, X. Kang, K.-K. Wong, and A. Nallanathan, ''Optimizing DF cognitive radio networks with full-duplex-enabled energy access points,'' IEEE Trans. Wireless Commun., vol. 16, no. 7, pp. 4683–4697, Jul. 2017.

[10] Etti Mathur and Manish Mathuria, "Unbreakable Digital Watermarking using combination of LSB and DCT", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017