ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Enhancement of Security Protection between Mobile Users and Media Storage for Multimedia Applications.

Sandeep Kumar Manchikanti*, and Veeramuthu Venkatesh.

School of Computing, SASTRA University, Thanjavur, Tamil Nadu, India.

ABSTRACT

Consistently immense measure of advanced pictures will be transmitted over the Internet in different applications between clients at diverse geographical places. The security and genuineness issues of advanced pictures are getting to be famous than at any other time in recent memory, because of the fast development of sight and sound and Internet innovation. The proposed work presents blend of Discrete Wavelet Transformation (DWT) and versatile dither adjustment quantization system utilizing a DSP Processor to insert the watermark for assurance amid web imparting. The blend of DWT and ADM methodologies expands the security, strength and subtlety and preserves the quality of hidden watermark during transmission. Finally the results show proposed methodology provides better accuracy to existing methods in terms of quality preservation which will be estimated with peak signal to noise ratio and percentage residual difference.

Keywords: Digital watermarking, DWT, invisible watermarking, ADM

**Corresponding author*

INTRODUCTION

The web will be an huge imparting framework for the computerized and mobile user [1-3] for its cheapness and capability. Likewise the pictures can be promptly imparted, effortlessly utilized, transformed and transmitted which causes significant issues like illegal utilization and control of advanced substance. Subsequently, there is the requirement for verification strategies to secure images [4-6] advanced pictures. Mobile devices such as smartphones organizes the world, and many people use to download/upload media stuff containing videos and pictures to remote servers. As mobile device has limited resources, and some media processing tasks must be migrated to the media storage for further processing. Many of the users may feel to hide their data from third parties and attackers. In case of defense organizations and crime investigation departments, sharing images or any information involves high secrecy and encrypted form. The robust security methods include cryptography [7-9] techniques and steganography techniques [10-12]. Cryptography techniques include light-weight encryption and decryption techniques for providing confidentiality. Steganography conceals secret information (file, message, image, and video) within other non-secret sources of same type. The proposed work falls under steganography, where confidential images or logos will be hidden in a non-secret video. In view of implementation, the proposed work makes use of digital watermarking [13-15] technique to hide his/her information, which is perceptually invisible. For the security of information there has been increasing curiosity in evolving operative procedures to dampen the unofficial duplication of digital information. Digital watermarking is the practice of embedding information into a digital signal in a way that is hard to eliminate. The invisibleness of watermark is identified with power of implanting watermark. Improved invisibleness is acknowledged for low quality watermark. So we must select the greatest force to embed watermark. A trade off will be there between implanting power (watermark strength) and quality (watermark intangibility). For a watermark to be robust, it should abide features such as imperceptible, readily extractable, robustness and definite.

- Imperceptible – It should not allow users to perceive the difference before and after applying watermark.
- Readily extractable – Authorized individual should able to extract hidden information easily.
- Robustness – It should resist any degree of attacks and changes.
- Definite – It should reveal the information on retrieval unambiguously.

The digital image watermarking pattern is of two types visible and invisible. Visible watermark meant to show copyright of owner on his information. In Invisible watermarking secret image or file with in non-secret image can't be seen thusly. The imperceptible watermarks are characterized into delicate and vigorous watermarking procedures. Delicate and semi-fragile methods are not feasible to rely as it fails to detect even slightest modification done to hide the secret information. A robust watermark technique can resist against selected class of alterations. In general a robust watermark helps to authorize owners copyright on his information. The proposed framework manages a strong watermarking. Most usually utilized applications include copyright related applications, medicinal legal, and substance confirmation applications.

The focal point of steganography over cryptography alone is that the recommended anonymous message does not pull in thoughtfulness regarding itself as an object of investigation. Obviously noticeable encoded messages—regardless of how unbreakable—will move investment, and may in themselves be implicating in nations where encryption is unlawful. Subsequently, though cryptography is the act of securing the substance of a message alone, steganography concerns with hiding the way that a mystery message is being sent, and in addition disguising the substance of the message.

A wavelet transform approached in proposed framework overcomes the disadvantages of existing transforms like Fourier transform. Wavelet means small wave. Wavelets are functions generated by single oscillatory function of finite duration by dilations and translation. Wavelet gives period occurrence localization of sign and the majority of the vitality of the sign are spoken to by a couple of development co-effective. The energy of a wavelet is unity. Wavelets are capacities that fulfill certain numerical prerequisites and are utilized to speak to information or different capacities. Wavelet applications are signal Defaming, watermarking, Detecting disentrances and breakdown focuses, Detecting comparability toward oneself, Compressing pictures, identifying pure frequencies, seismic and geophysical signal processing and video compression.

Related Works

The two classifications of Digital watermarking calculations are spatial-area methods and recurrence space strategies. Slightest Significant Bit (LSB) will be the gaudy method in the spatial area systems which straight away changes the intensities of around specific pixels. The recurrence area procedure changes a picture into an arrangement of recurrence space coefficients. The change received may be discrete cosine change (DCT), discrete Fourier changes (DFT) and discrete wavelet changes (DWT) and so on. In the wake of applying change, watermark is inserted in the changed coefficients of the picture such that watermark is not unmistakable. At last, the watermarked picture will be acquired by obtaining converse change of the coefficients.

The limitations of DCT are blocking artifacts, graininess, blurring. Blocking artifact is like image after recovering will look like blocks rather than like original image, from one block to another block variations occur. Graininess is due to truncation of low frequency components and lack of information. In the proposed framework, watermarking is implemented based on discrete wavelet change. Wavelet change is a proficient instrument to speak to a picture. The wavelet change permits multi-determination examination of a picture. A wavelet transform can be broadly classified into (i) continuous wavelet transform, and (ii) discrete wavelet transform. Discrete wavelet changes can be executed through sub-band coding. The DWT is helpful in picture handling in light of the fact that it can at the same time limit motions in time and scale, while the DFT or DCT can restrict flags just in the recurrence space. A Fourier change does not give data about the time at which a specific recurrence has happened in the signal. Subsequently a Fourier change is not a compelling apparatus to break down a non-stationary signal. The wavelet change gives a period recurrence representation of a sign. The wavelet change was produced to conquer the deficiencies of the brief time Fourier change, which can be utilized to investigate non-stationary signals. The principle downside of the STFT is that it gives a steady determination at all frequencies, while the wavelet change utilizes a multi-determination method by which diverse frequencies are broke down with distinctive resolutions. The fundamental thought of the wavelet change is to speak to the signal to be examined as a superposition of wavelets.

The DWT is gotten by sifting the sign through a progression of computerized channels at distinctive scales. The scaling operation is carried out by changing the determination of the sign by the process of subsampling. The original image which is going to be hidden in cover image will be digitally watermarked using discrete wavelet transform. In this scheme watermark is generated from host image content that has to be hidden, then using discrete wavelet transform it is embedded in to cover image. The discrete wavelet transform is different from other transforms in its functionality. It is preferred over many frequency transforms, because when a low frequency is generated it will be difficult to find when and where occurred using existing transforms. In DWT it is all about localization i.e. space-frequency localization. It helps to analyze at which location we will have higher frequency components and at which location we will have lower frequency components. DWT can also be implemented through (i) filter bank scheme, or (ii) lifting scheme.

Implementation

The wavelet change deteriorates a picture into an arrangement of diverse determination sub-pictures, relating to the different recurrence groups. This outcomes in a multi-determination representation of pictures with restriction in both the spatial and recurrence spaces. This is attractive on account of picture pressure, however it is impractical on account of Fourier and cosine changes which gives great confinement in one space to the detriment of other. The main advantage of wavelet based image compression is:

- Wavelets have non-even recurrence spectra which encourage multi-scale investigation
- Multi-resolution property of the wavelet transform can be used to exploit the way that the response of the human sense is different to high and low frequency components of an image
- DWT can be applied to an entire image without block structures as used by the DCT, thereby reducing blocking artifact

In the proposed framework, there will be three essential sections: Watermark generation, Watermark inserting and Watermark Detection. Watermark is made taking into account pixel estimations of genuine picture. Watermark is performed using 1-level Discrete Wavelet Transform. In proposed frame work sub-band coding helps to divided the input signal into several frequency bands. The following figure 1 shows a wavelet decomposition in-depth.

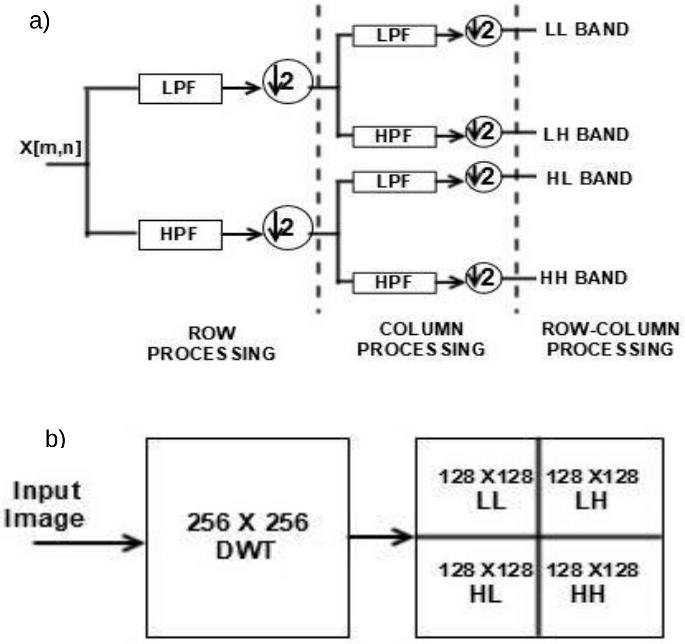

Figure 1: Wavelet Decomposition

Fig 1.a shows a row and column wise decomposition involves low pass and high pass filter with decimation level and Fig 1.b shows the result of wavelet decomposition with corresponding size and various generated frequency bands. A picture can be assessed by disregarding an investigation channel level tailed by annihilation activity. The investigation channel gathering includes a low-pass and high-pass channel on partitioned deterioration stage. At the point when a sign goes through these channels, it ruptures into two groups. The low pass channel identifies with averaging process that concentrates unpleasant information of sign. The high pass channel relates to differencing process that extracts detailed data of signal. The yield of the sieving procedure is then demolished by two. A two-dimensional change is fulfilled by executing two different one-dimensional changes. Initially, the picture is perplexed along the column and wrecked by two. It is then tailed by separating the sub-picture along the segment and annihilated by two. It is then tailed by sifting the sub-picture along the segment and wrecked by two. The operation parts the picture into four groups, to be specific LL, LH, HL and HH separately. This method of partitioning is called Dyadic partitioning. To obtain robust watermark of original image, it is embedded in to HH sub-band having high frequency signals such that it should stand against several attacking filters designed by attackers. The resultant image is called watermarked picture. In discovery stage, two sorts of watermarks will be acquired. One is created from watermarked picture and the other is separated from HH1 sub-band which has been as of now installed inside the host picture. Examination is made between those watermarks to choose realness. The generated watermark must be perceptually same as of original cover image, so that attacker will skip the content believing it as normal content.

Hardware Description

Hardware implementation is based on TMS320C6745, a fixed and floating point digital signal processor. A higher end processor supports versatile libraries to program, includes cache memory, RAM and flexible ROM. Code Composer Studio contains a suite of instruments used to create and investigate inserted applications. It incorporates an advancing C/C++ compiler, source code supervisor, task fabricate environment, debugger, profiler, and numerous different peculiarities. CCS debugs the code written in C language. Input is a video of audio-video interleave (avi) format. The secrete image is hidden in one of the frames of the video, to provide robustness against attacks. A procedural steps helps an individual to create an executable file using code composer studio IDE that runs on the hardware. The flow of execution on hardware is demonstrated in the following figure 2.

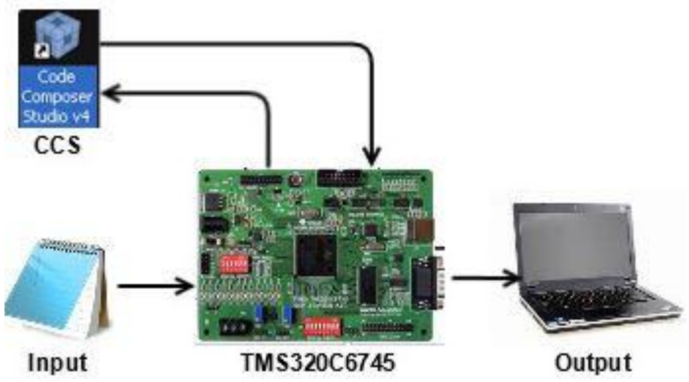

Figure 2: Implementation on DSP Controller

Figure 2 clearly explains that input image frame is given in pixel format stored in a notepad and is included as header file in the program written for execution on hardware. The implementation output is visualized with a PC installed with code composer studio. The following figure 3 depicts the flow of the watermark generation and embedding of the watermark in to the selected frame of the selected sub-band frequency.

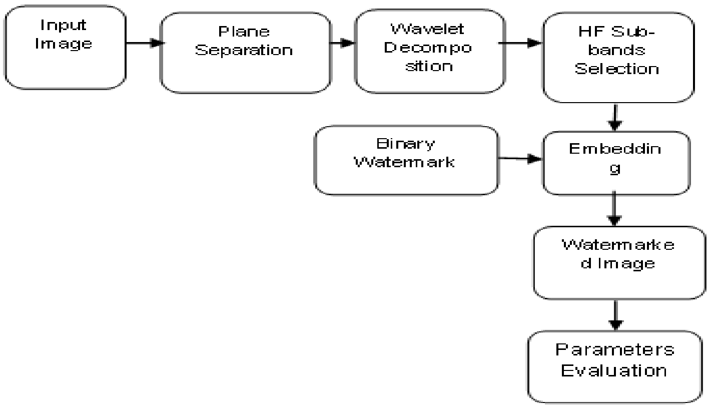

Figure 3: Watermark embedding process

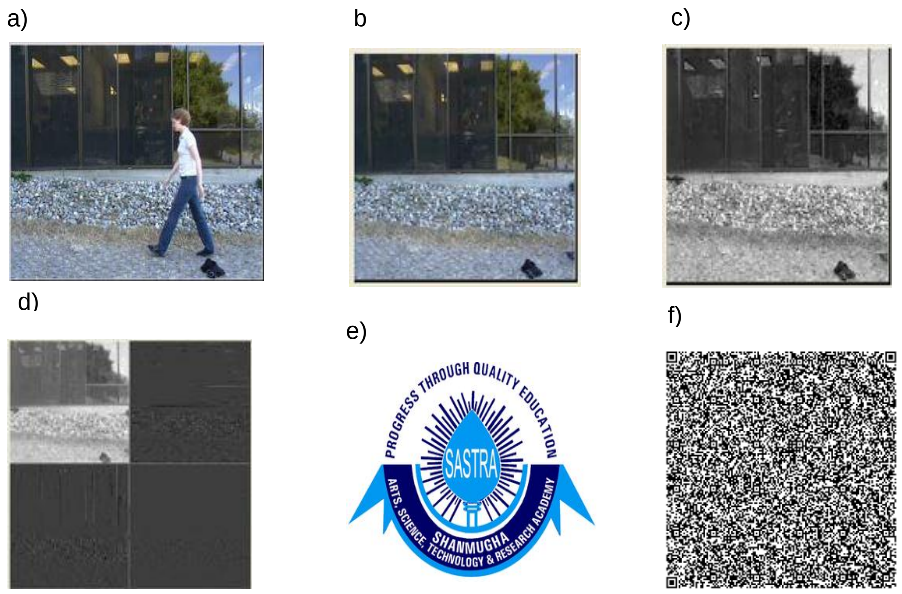
a)
b
c)
d)
e)
f)
PROGRESS THROUGH QUALITY EDUCATION
SASTRA
ARTS, SCIENCE, TECHNOLOGY & RESEARCH ACADEMY
SHANMUGHA

Figure 4: Pictorial depiction of blocks in flow diagram

Figure 4 depicts the pictorial representation of the flow chart representing the process of watermarking. Figure 4.a represents the original video i.e. cover video. Figure 4.b is selection of the frame of embedding process. Figure 4.c is the frame or plane seperation process. Figure 4.d depicts the wavelet decomposition for sub-band selection. Figure 4.e shows a secret image that is to be watermarked and transmited secretly. Figure 4.f is a watermarked image obtained after embedding of secret image with the selected sub-band. The image to be hidden is transformed in to binary to restore the actual pixlar value of the cover image even after embedding the secret image. This is done with a preloaded image and preloaded video in ot the storage space of hardware.

The extraction process is exactly reverse of the generation and embedding of watermark. The extraction should be very robust in such a way that any of the attackers cannot be able to decode the image hidden with any kind of the filter designed. A user must have calculated values of the parameters such as peak signal to noise ration and mean square error of the images so that during the extraction process, one should confirm that the extracted secret image is not tampered or altered by any external attacker. This kind of authenticity is mostly invited by many media storage mediators for proving protection to the users information which have to be kept secretlyduring sharing between users through internet. Figure 5 depicts the extraction process of the watermark.

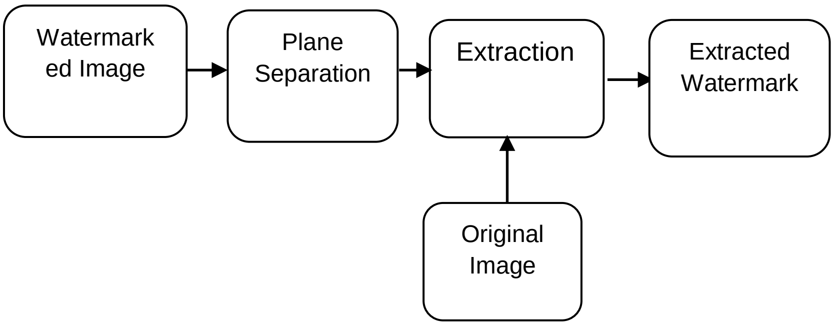

Figure 5: Watermark detection and extraction

The adaptive dither modulation technique is implemented along with the dwt. Dithering is the process of adding random noise to a signal before reducing its bit depth. The noise in the sense its good noise, which is white noise. Dithering helps to get rid of quantization noise. An example of dithering is a originally recoreded audio of 24bits is ditered and downsampled to 16bit while releasing to market in form of CDs which is noise free. The ADM along with DWT plays a vital combination in restoring the extracted image quality. An input image to that white noise is added and downsampled to desired bit depth and output is obtained. The image can be further modified or improved by calculating the white noise value obtained on subtraction of input image with dithered image.

The parameters such as peak signal to noise ration and percentage residual difference. Crest sign to-commotion proportion, habitually truncated PSNR, is a term for the degree between the amazing likely force of a sign and the force of adulterating clamor that influences the loyalty of its representation. Since numerous signs have a wide dynamic reach, PSNR is for the most part explained as far as the logarithmic decibel scale. PSNR at max simply distinct by the mean squared error (*MSE*).

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

Where $\mathrm{MAX}_{\mathrm{I}}$ is the maximum probable pixel estimation of the picture, when the pixels are spoken to utilizing 8 bits every specimen, this is 255. The above mentioned equation (1) supports in calculating the PSNR and MSE value for different approaches.

RESULTS AND DISCUSSION

The values obtained calculated with the above mentioned formulae for DWT for MSE and PSNR are:

PSNR = 77.4661 db

MSE = 0.001165

The PSNR must always be as high as possible, because it represents the preceptuality of the image when it is extracted. The existing methods shows very poor values that are less than half of values obtained for DWT. Hence DWT was preferred over existing methods for image hiding. It is a low distortion and flexible process and watermark will be protected from invariatnt features. The robustness provided by the proposed technique enhances the security for application like copyright protection and in defense systems.

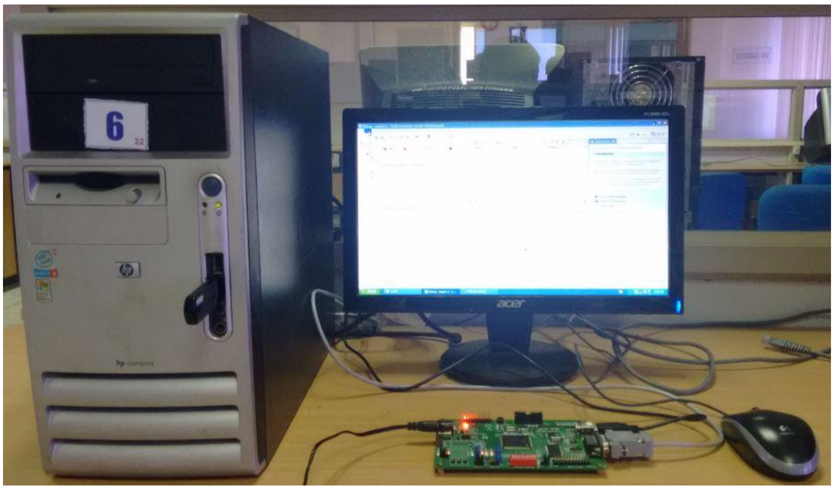

Figure 6: overall system setup

CONCLUSION

Security protection between user and media storage is demanded more in future for multimedia applications. In this structure, a joint outline of computerized watermarking taking into account discrete wavelet change with versatile dither adjustment for denoising. This system has given another vigorous watermarking plan, which manages an entirety system that inserts and identifies the watermark data productively. The watermark installing methodology does not wreck the visual prominence of the picture. The pointed technique uses Discrete Wavelet Transform which manages a recurrence range of the watermark inside the host picture. Besides the acceptance procedure offers qualities like intangibility, strength and security.

ACKNOWLEDGEMENT

This work was supported by FIST programme, Department of Science and Technology, India, Grant no: SR/FSC/ETI-371/2014 at SASTRA University, Tirumalaisamudram, Thanjavur

REFERENCES

[1] Nadembega.A,Hafid.A&Taleb.T, “An integrated predictive mobile-oriented bandwidth-reservation framework to support mobile multimedia streaming”,IEEE Transactions on Wireless Communications, 2014, 13(12), 6863-6875.

[2] Felemban.M,Basalamah.S&Ghafoor.A,”A distributed cloud architecture for mobile multimedia services”, IEEE Network, 2013, 27(5), 20-27.

[3] Ahmad.I& Gabbouj.M, “A generic content-based image retrieval framework for mobile devices”, Multimedia Tools and Applications, 2011, 55(3), 423-442.

[4] Muhaya, F. B., Usama, M., & Akhter, F, “ Chaos based secure storage and transmission of digital medical images”, Applied Mathematics and Information Sciences, 2014, 8(1 L), 27-33.

[5] Al-Khassaweneh.M.& Tawalbeh.S, “A value transformation and random permutation-based coloured image encryption technique”, International Journal of Information and Computer Security, 2014, 5(4), 290-300.

[6] Pande.A,Mohapatra.P & Zambreno.J, “Securing multimedia content using joint compression and encryption”, IEEE Multimedia, 2013, 20(4), 50-61.

[7] Chen.C, Chen.W,Chen.C, Lai.Y& Tseng.K, “ A secure visual secret checking of meaningful sharing images”, Applied Mathematics and Information Sciences, 2014, 8(5), 2327-2335.

[8] Yeh.L & Tsaur.W, ”A secure and efficient authentication scheme for access control in mobile pay-TV systems”, IEEE Transactions on Multimedia, 2011, 14(6), 1690-1693.

[9] Ismail.I, A.Amin, & Diab.H ,”A digital image encryption algorithm based a composition of two chaotic logistic maps”, International Journal of Network Security, 2010,11(1), 1-10.

[10] Thanikaiselvan.V,Subashanthini.S&Amirtharajan.R, “PVD based steganography on scrambled RGB cover images with pixel indicator”, Journal of Artificial Intelligence,2014, 7(2), 54-68.

[11] Amirtharajan.R, Ashfaaq.M.K, Infant.K.A, & Rayappan J.B.B, “ High performance pixel indicator for colour image steganography”,Research Journal of Information Technology, 2013, 5(3), 277-290.

[12] Mohd.B.J, Hayajneh.T & Quttoum.A, “ Wavelet-transform steganography: Algorithm and hardware implementation”, International Journal of Electronic Security and Digital Forensics,2013, 5(3-4), 241-256.

[13] Huang.D, Hung.K,Hou.T & Chan.Y, “A secret communication method based on watermarking technique using genetic algorithm”, Journal of Internet Technology, 2015, 16(1), 85-93.

[14] Bhatnagar.G,JonathanWu.Q.M & Atrey.P.K, “Robust logo watermarking using biometrics inspired key generation”, Expert Systems with Applications, 2015,41(10), 4563-4578.

[15] Kannammal.A & SubhaRani.S, “Two level security for medical images using watermarking/encryption algorithms”,International Journal of Imaging Systems and Technology, 2015, 24(1), 111-120.