THE DICOM 2013 INTERNATIONAL CONFERENCE & SEMINAR
March 14-16 Bangalore, India

An Overview of Digital Watermarking & Data Hiding Techniques for Secure Transmission of Medical Images

K. ANUSUDHA

Assistant Professor

Department of Electronics Engineering,

Pondicherry University,

Pondicherry, India.

Content

Research Aim

The main focus is to provide secure medical image transaction as the exchange of "medical reference data" done via unsecured open networks leads to the condition of changes to occur in medical images and creates a threat which results in undesirable outcome.

Origin of the Problem

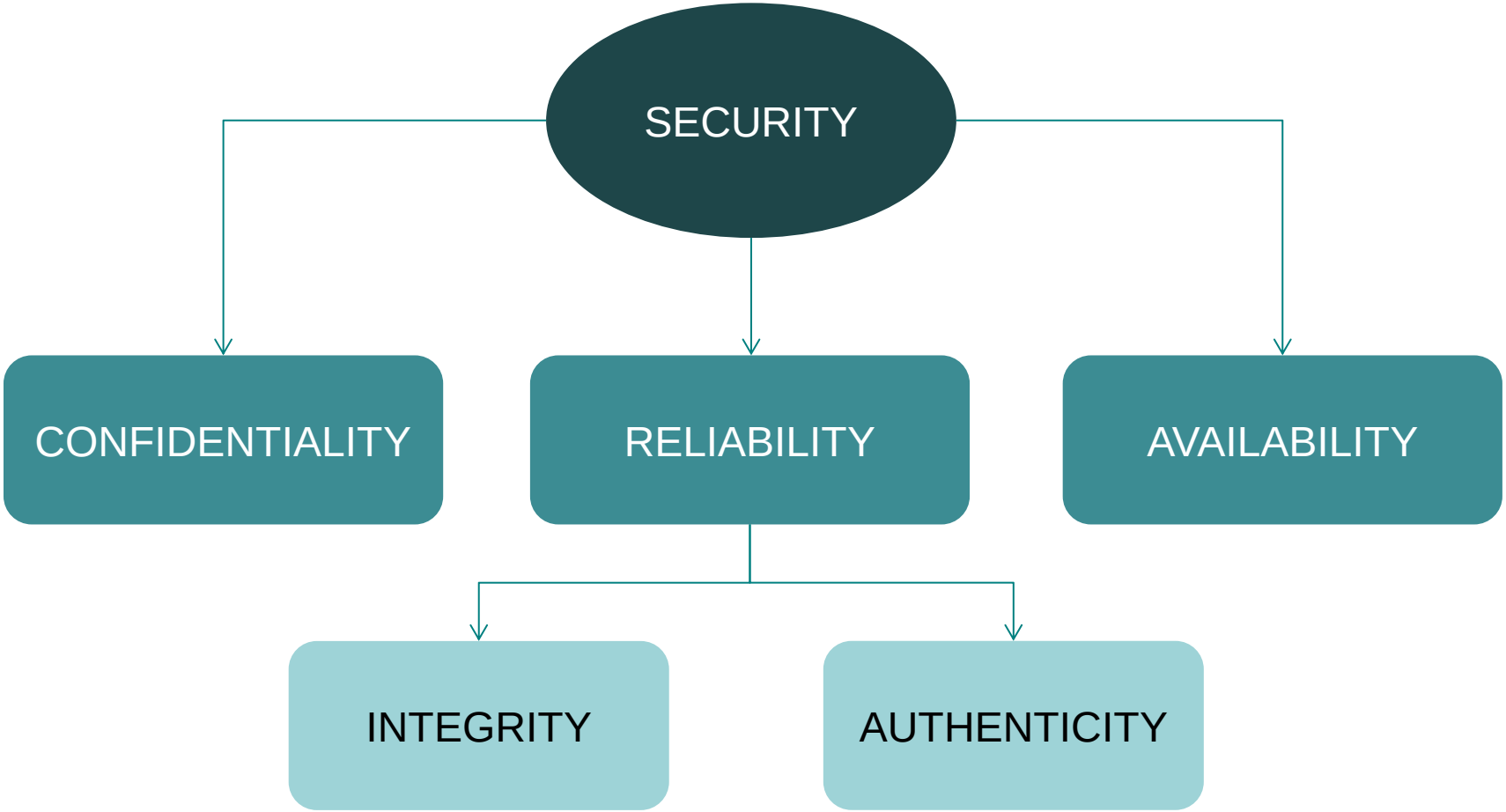
- **Modern Health care Infrastructure.**
- **Easy access of medical information.**
- **Maintenance of Electronic Health record.**
- **Sheer amount of database.**

Need for Medical Image Security

To avoid:

- **False insurance claim.**
- **Distribution of famous persons reports to tabloids.**
- **Misinterpreted Telediagnosis results.**
- **Escaping from crime.**

Components of Medical Image Security



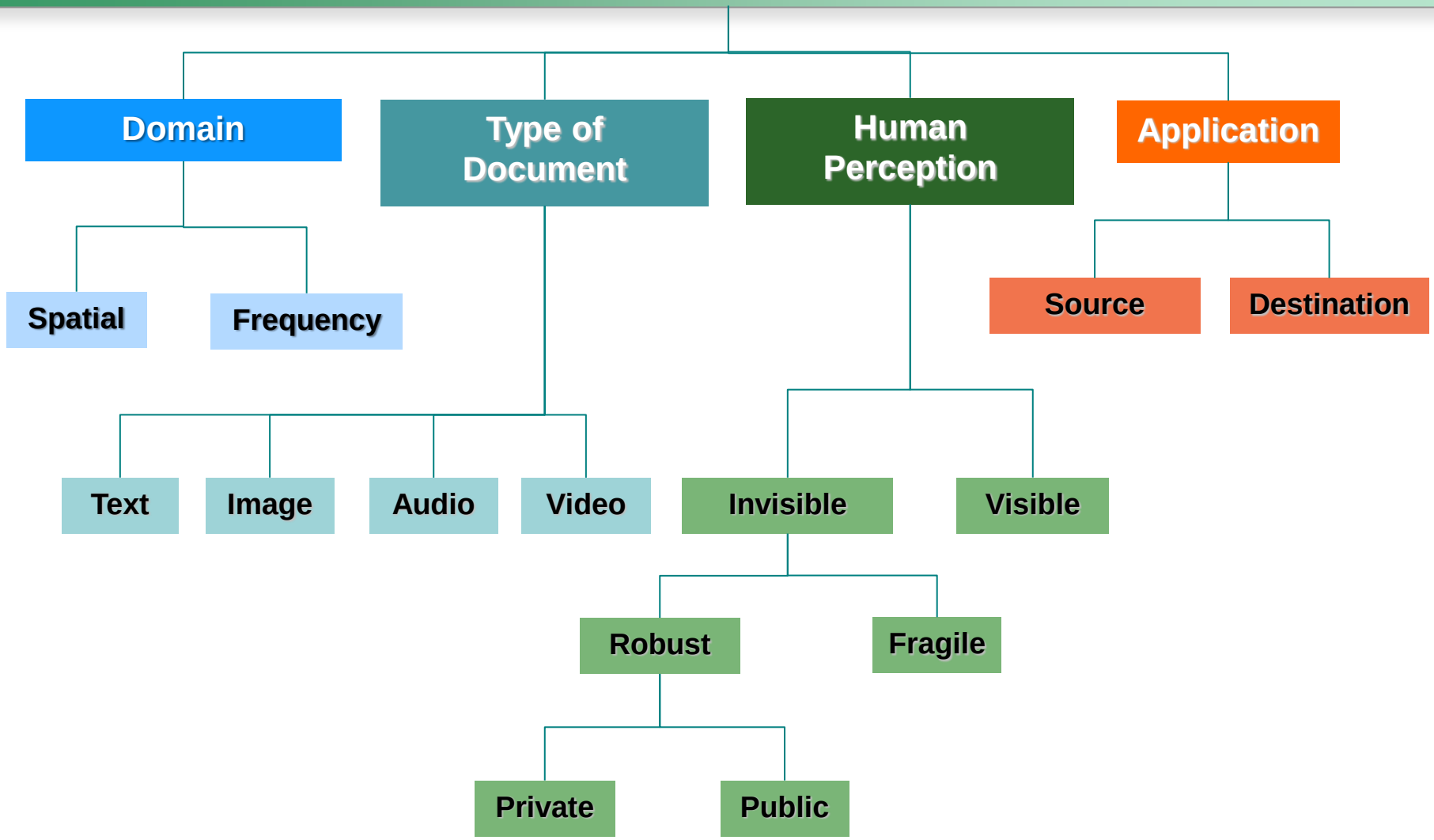
Digital Watermarking Technique

Digital watermarking is a steganographic technique which concentrates on providing authentication, copyright protection and ownership identification.

Features:

- ✓ **Imperceptible**
- ✓ **Robust**
- ✓ **Oblivious/Non-oblivious**
- ✓ **Payload size**

Classification



Relevance

- **Cover Content:** **Medical Data**
- **Secret message:** **EPR, Doctors ID, Hospital logo, UIN.**
- **Domain:** **Spatial & frequency**
- **Types:** **ROI/RONI based**

Data Hiding Technique

Cryptographic techniques can be combined with Digital watermarking to increase the level of security.

Features:

- ✓ **Key generation**
- ✓ **Computational efficient**

Performance Metrics

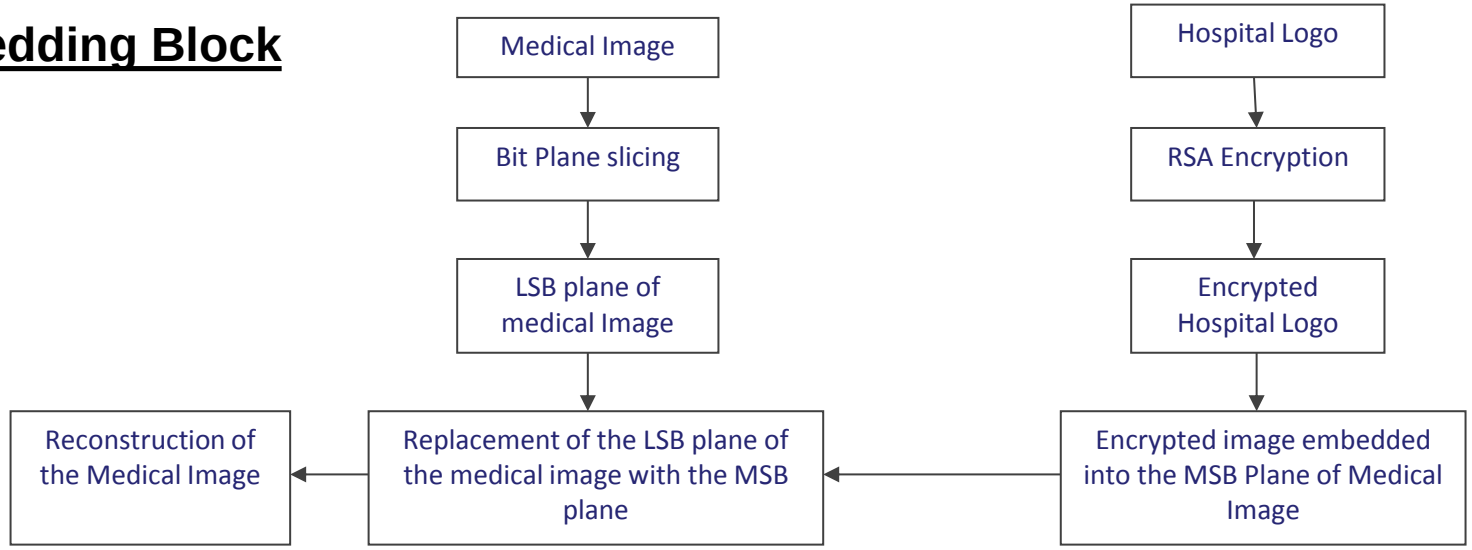
Mean Square Error (MSE)	$\left(\frac{1}{n^2}\right)\sum\left(I - I^*\right)^2$
Peak Signal to Noise Ratio (PSNR)	$10\log_{10}\left(\frac{\max\left(I^2\right)}{MSE}\right)$
Image Fidelity (IF)	$1 - \frac{\sum\left(I - I^*\right)^2}{\sum I^2}$
Number of Pixels Change Rate (NPCR)	$\frac{\sum^{i,j} D(i,j)}{W \times H} \times 100\%$
Unified Average Changing intensity (UACI)	$\frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{2^L - 1}\right]$

SCHEME I

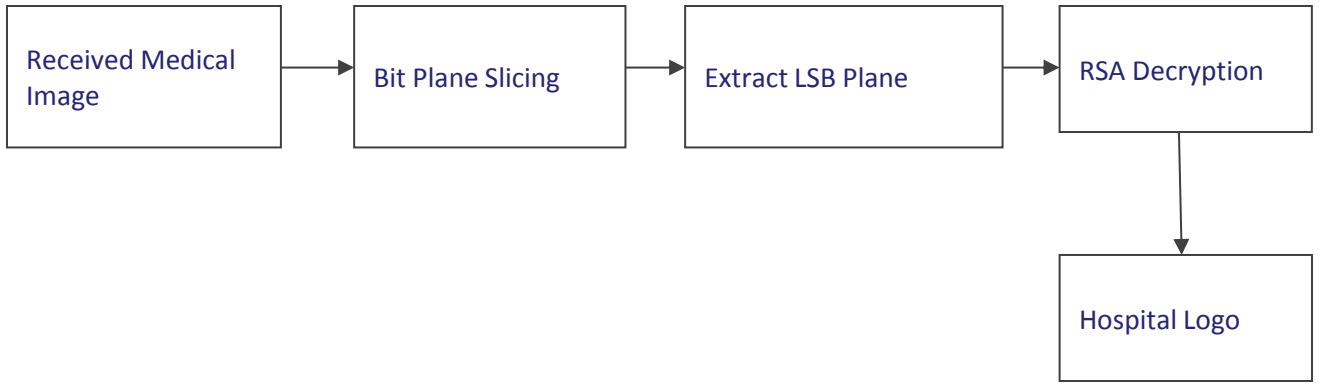
SELECTIVE PLANE REPLACEMENT WATERMARKING

Proposed Block Diagram

Embedding Block



Extraction Block



Embedding Process - Algorithm

Step 1: The input medical image undergoes bit plane slicing. Image is partitioned to eight planes (LSB-MSB).

Step 2: Hospital logo is considered as the secret image and is the input for RSA encryption.

Step 3: The secret image is then encrypted using the RSA encryption method,

$$C=M^e \bmod n$$

where: C - Encrypted image, M - Secret image e - Public key and

n - Multiplicand of prime numbers (p,q)

Step 4: The encrypted image bits replaces the MSB plane bits of the Medical image.

Step 5: The MSB plane is replaced in place of the LSB plane of the medical image.

Step 6: All the planes are reconstructed back to form the Secured Medical image.

Extraction Process - Algorithm

Step 1: The received Medical image is passed on for Bit plane slicing.

Step 2: The LSB plane is recovered and applied for RSA decryption.

Step 3: The secret message is retrieved from the LSB plane using the RSA decryption method, where

$$M = C^d \bmod n$$

Where: C - Encrypted Image

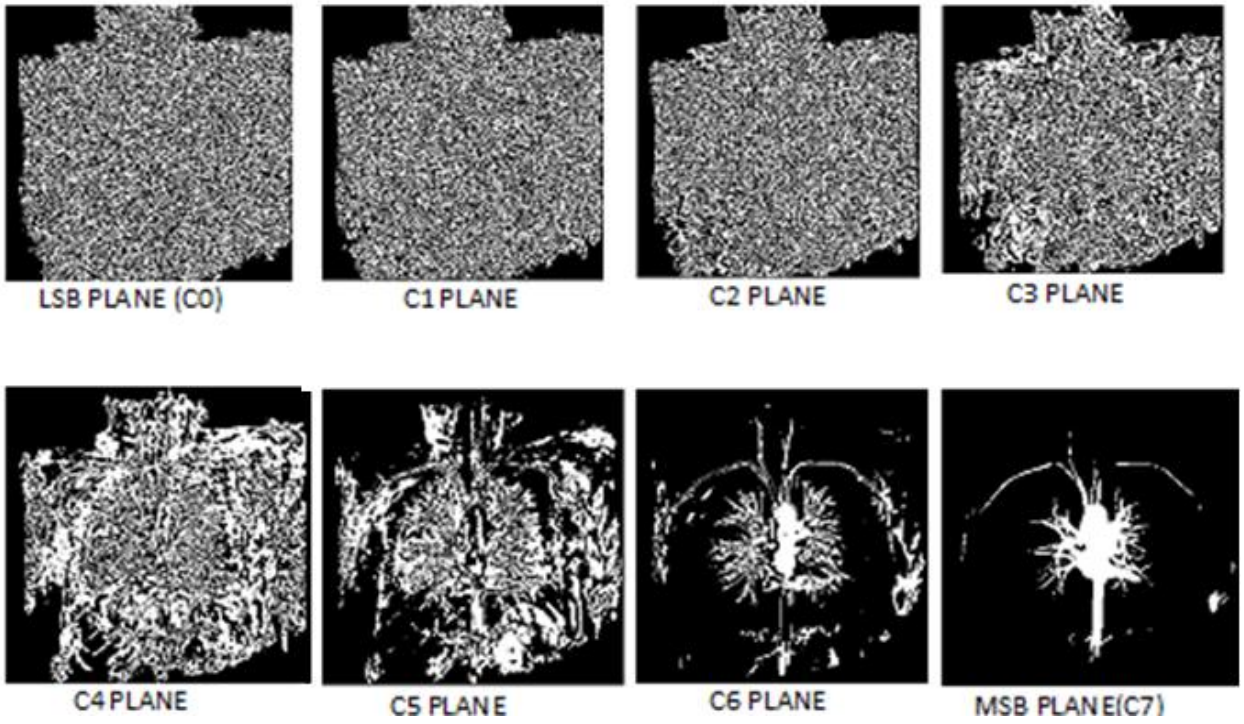
d - Private Key

Simulation Results

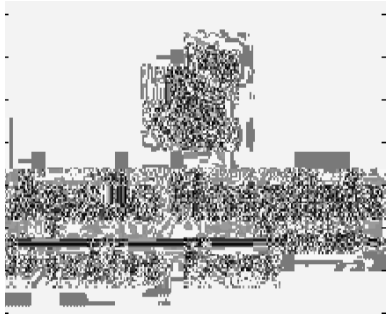
CT Image (512x 512)

Hospital Image (221x228)

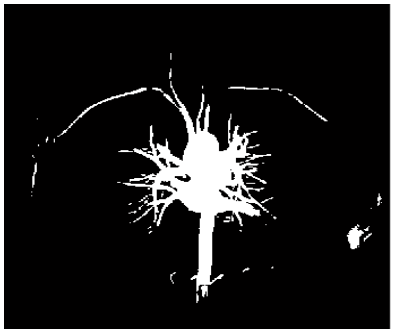
Simulation Results



Bit Plane Slicing of CT image

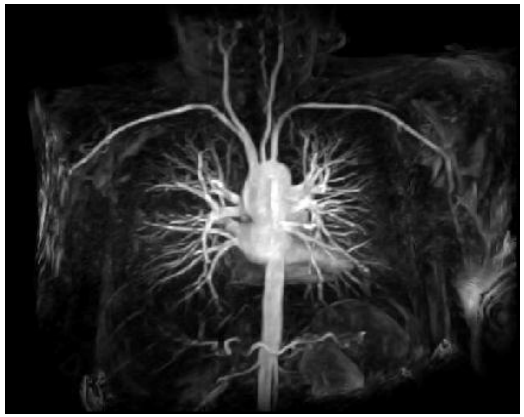


Encrypted Hospital Image

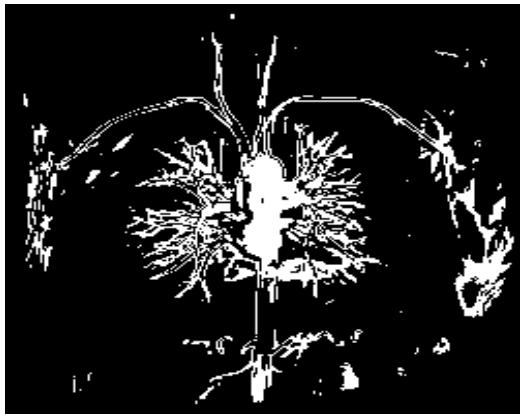


Data hided MSB plane of CT Image

Simulation Results



Reconstructed CT Image

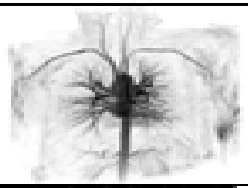
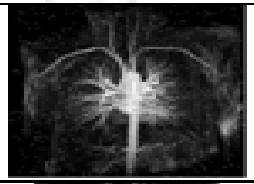
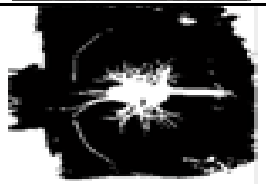
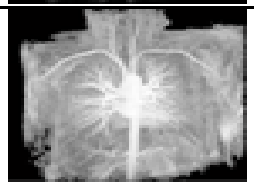
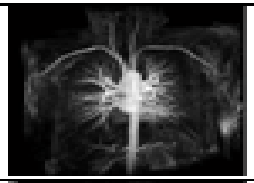
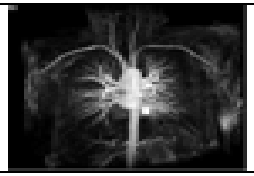


Recovered LSB plane

Apollo Hospitals GROUP
touching lives

Decrypted Hospital logo

Performance Analysis

ATTACKS	IMAGES	MSE	PSNR (dB)
Negative Transform		0.7964	49.1197
Noise Attack (Salt & Pepper) 0.2 0.4 0.6 1		 0.2592 0.3174 0.3774 0.5005	 53.9951 53.1151 52.3630 51.1364
Rotation 45° 60° 90°		 0.5186 0.5591 0.6946	 50.9824 50.6561 49.7862
Smoothening		0.3543	52.2643
Gamma correction 0.6 0.4 0.2		 0.0723 0.1404 0.3032	 59.5379 56.6564 53.3131
Contrast Stretching		0.2053	54.5412
Cropping		0.1432	54.1342

Merits of Scheme I

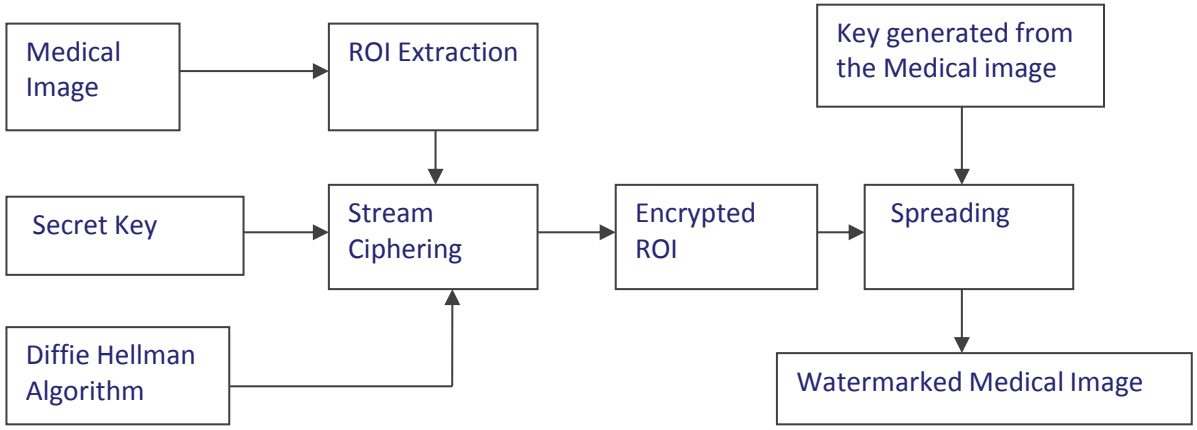
- **Can be applied for all types digital Medical Images.**
- **Size of the payload is flexible.**
- **ROI of the image is not disturbed.**
- **Withstands various attacks.**

SCHEME II

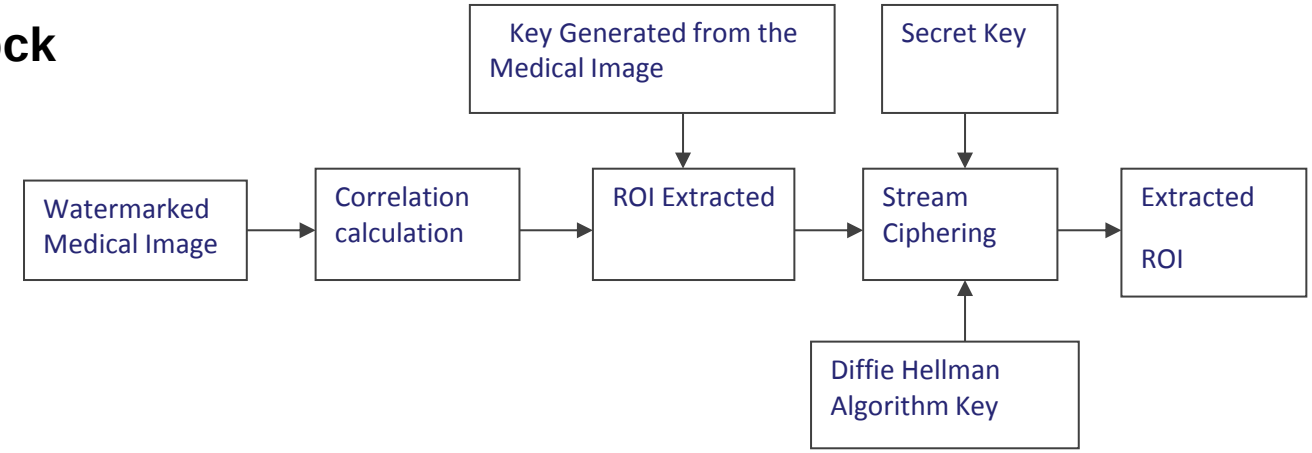
STREAM CIPHERED SPREADING WATERMARKING

Proposed Block Diagram

Embedding Block



Extraction Block



Embedding Process - Algorithms

Step 1: ROI portion is extracted from the medical image.

Step 2:64 bit - PRNG sequence is generated and the bit stream is divided into groups of eight bits to form eight 8 bit key sequences.

Step 3: The ROI portion is divided into 8x8 blocks and each pixel is multiplied with the 8 bit key sequences and encrypted using stream ciphering technique .

Step 4: The same 64 bit random binary sequence is used for generating the Diffie Hellman Key generation.

Step 5: The key generated by the Diffie Hellman algorithm is added to every encrypted stream ciphered pixel Values thereby the Encrypted portion of ROI is obtained which acts as the Watermark.

Step 6: A pseudo random key generated from the medical image is used for spreading the encrypted watermark on to the medical image to generate the watermarked medical image.

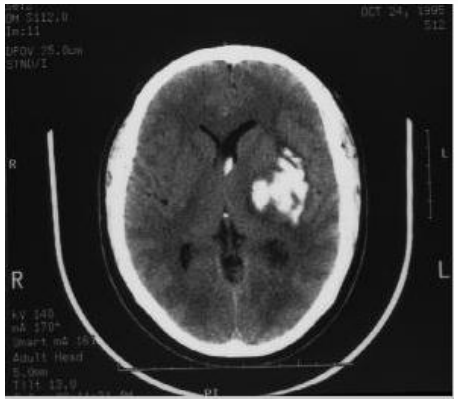
Extraction Process - Algorithms

Step 1: The correlation between the received watermarked image and the Pseudo random sequence is calculated.

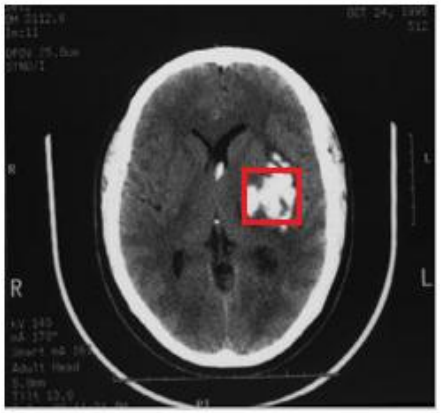
Step 2: The correlation value is used as the threshold for despreading the watermark.

Step 3: The obtained watermark is decrypted by the Diffie-Hellman algorithm key and the 64 bit sequence.

Simulation Results

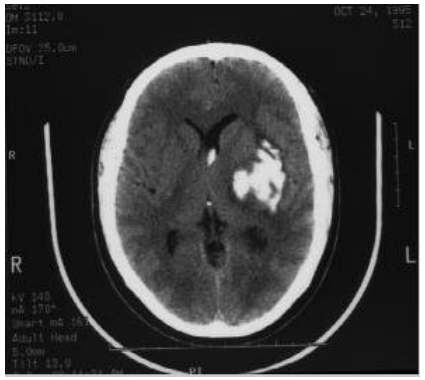


MRI Image (512x512)

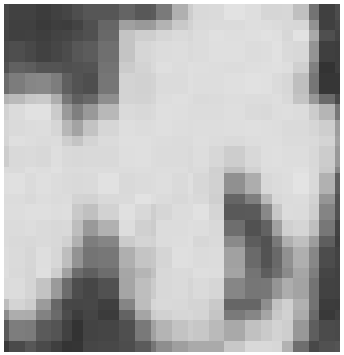


ROI portion of the Cover image

encrypted ROI

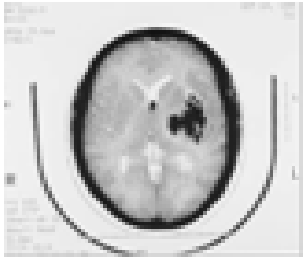
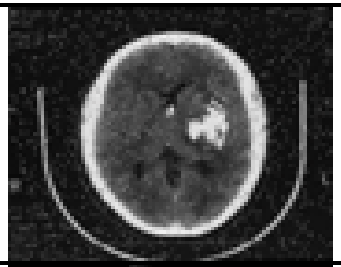
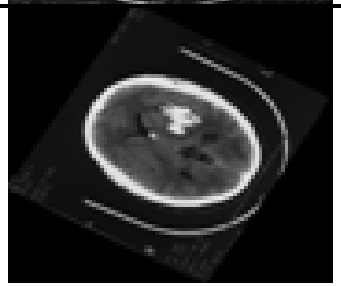
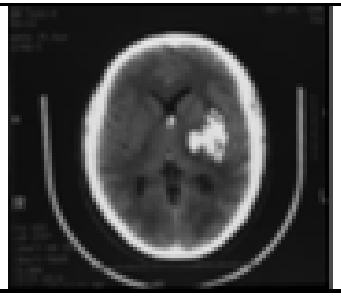


Watermarked MRI image

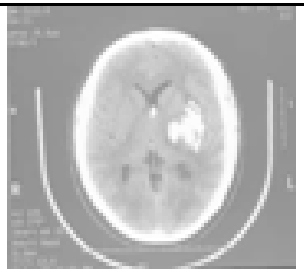
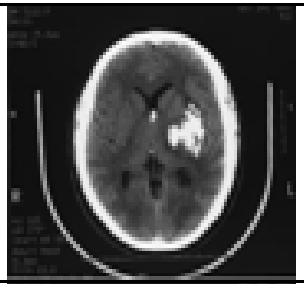
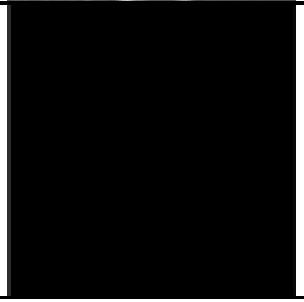


Zoomed retrieved ROI from the watermarked Image

Performance Analysis

ATTACKS	IMAGES	MSE	PSNR (dB)
Negative Transform		0.2567	54.2315
Noise Attack (Salt & Pepper) 0.2 0.4 0.6 1		 0.3001 0.3210 0.3210 0.5915	 54.2540 53.1151 52.5640 50.0976
Rotation 45° 60° 90°		 0.2965 0.3174 0.4978	 54.9824 53.6561 51.7862
Smoothening		0.3224	53.1432

Performance Analysis

ATTACKS	IMAGES	MSE	PSNR (dB)
Gamma correction 0.6 0.4 0.2		 0.3120 0.3967 0.4328	 55.1245 53.4645 50.3131
Contrast Stretching		0.4367	50.2145
Cropping		0.2762	54.2435
Fidelity		Parameter of Human visual system	

Merits of Scheme II

- **Can be applied for any Medical Image.**
- **ROI is ciphered to act as the watermark.**
- **Payload size is flexible.**
- **Withstands various attacks.**

Key Issues

- **Size of the payload**
- **Region based algorithms**
- **Withstand all types of Image processing attacks**
- **High fidelity**

Conclusion

The approach of providing security to medical images by combining Digital watermarking and data hiding techniques is an added feature to the distribution of DICOM standard images.

References

1. V. Fotopoulos, M. L. Stavrinou, A. N. Skodras, "Medical Image Authentication and Self-Correction through an Adaptive Reversible Watermarking Technique", IEEE Transaction on Bio-Informatics and Bio-Engineering , pp. 1-5, October 2008.
2. H.-K. Lee, H.-J. Kim, K.-R. Kwon, J. K. Lee, "ROI Medical Image Watermarking Using DWT and Bitplane", ACM Journal on Image Computing, 3-5, October 2005.
3. Cao, F., Huang, H.K. and Zhou, X.Q., “Medical image security in a HIPAA mandated PACS environment. Computerized Medical Imaging and Graphics”, IEEE transaction on Image Processing **27**(2-3), pp. 185-196, 2003.
4. Zkou, X.Q., Huang, H.K. and Lou, S.L., “Authenticity and integrity of digital mammography images”. IEEE Transactions on Medical Imaging, **20**(8), pp. 784-791, 2001.
5. Chao, H.M., Hsu, C.M. and Miaou, S.G.,”A data-hiding technique with authentication, integration, and confidentiality for electronic patients records”, IEEE Transactions Information Technology in Biomedicine, **6**, pp. 46-53, 2002.
6. Wang Yan and Ling-di Ping, “A New Steganography Algorithm Based on Spatial Domain”,Journal on Information Science and Engineering ,vol 6,45-51,2009.
7. Ran –Zan Wang, Chi-Fang Lin, Ja Chen Lin, “Hiding data in images by optimal moderately significant bit replacement” Pattern Recognition, Vol 3, pp 671-683, 2001.
8. Chi-Kwong Chan et al,” Hidden data in images by simple LSB substitution”, Elsevier Pattern Recognition, Vol 37,pp 469-474,2004.
9. Chin Chen Chang et al ,” A watermarking based image ownership and tampering authentication scheme” Pattern recognition letter Vol 27,pp 439-446,2006.
10. Dalel Bouslimi et al, “A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images”, Computer methods and programs in biomedicine, Vol 106, pp 47-54, 2012.
11. Mustafa Ulutas, Guzin Ulutas and Vasif , “Medical Image security and EPR hiding using Shamir’s secret sharing scheme”, ACM Journal of systems and software ,vol 84, pp 341-353,2011.

Author Contacts

K. Anusudha

E-mail: anusudhak@yahoo.co.in,

anusudha.dee@pondiuni.edu.in

Department of Electronics Engineering,

Pondicherry University.

N. Venkateswaren

E-mail: venkateswarann@ssn.edu.in

Department of ECE,

SSN College of Engineering.

Thank you for your attention!!!