Robust Embedding of Patient ID in Medical Images for Telemedicine Applications

Sunita V. Dhavale
Department of Computer Engineering, Defense Institute of Advanced Technology, Pune – 411025, INDIA.
sunitadhavale75@hotmail.com

***Abstract*-** **Most of the researchers have been researching algorithm to insert high information in the original medical image but increasing the size of embedded information affects the quality of watermarked medical image severely. This paper presents a new robust image barcode watermarking scheme for medical images that embeds human readable bar-coded watermark image which is generated from corresponding unique patient identification number (PID). Here only PID barcode image is embedded in a medical image for telemedicine applications instead of embedding whole Electronic Patient Record (EPR) data. Further, the presence of PID barcode watermark can be identified with or without manual intervention. A PID sequence watermark is represented as bar-coded binary logo image and embedded in the corresponding medical image. This in turn authenticates corresponding medical images and also helps in faster retrieval of whole patient data from the centrally managed hospital database. The proposed scheme first extracts the energy of DCT blocks from the host image and based on these energy values, the blocks are then classified into two clusters named High Energy Blocks (HEBs) and Low Energy Blocks (LEBs) using KMeans clustering technique. To achieve imperceptibility, the watermark bits are embedded only in HEBs leaving LEBs intact. By using the desirable characteristics of proposed technique, the imperceptibility requirements of watermarks are fulfilled along with increased robustness. Experimental results show that the proposed scheme is robust against common attacks and offers both objective as well as subjective watermark detection. The revealed watermark can be easily recognized by human eyes, even if the host image has undergone severe attacks. Due to inherent error detecting capability of the barcode watermark image, the watermark can be fully recovered against various kinds of attacks.**

Keywords - Digital watermarking; Medical image; Robust; K-Means; DCT.

I. INTRODUCTION

Telemedicine application requires transferring medical images over network for further diagnostic purpose [5]. Using digital watermarking in case of telemedicine can verify authenticity as well as provide copyright protection for corresponding medical images [2, 3, 4]. Digital watermarking technology can embed some kind of digital information into multimedia data (such as image, sound etc.) mostly in invisible manner, which can provide copyright protection as well as authentication of the multimedia data and the information [3, 9]. The watermarking algorithms addressing a wide variety of applications can be classified into two main categories. The first category of algorithms uses a pseudo random gaussian sequence (PRGS) watermark where the presence of the embedded watermark is detected by using statistical correlation whereas the second category of algorithms use a binary logo as a watermark and this logo is extracted to detect the presence of watermark [1]. The former approach is more objective as it relies on a statistical correlation value to ascertain the presence of watermark however the latter approach is more subjective because the presence of watermark is detected by visual inspection by a third entity [1].

For better watermark detection, we must offer both subjective and objective detection simultaneously in one watermarking scheme. This approach provides an alternative detection mechanism in case the objective detection fails or is considered incorrect [1]. In order to address these issues we have used bar-code watermarking that represent the PID in a human readable bar-coded binary logo in order to offer both objective watermark detection using correlation and subjective watermark detection in case the objective detection fails. The extracted watermark can be visually inspected to extract the embedded PID number. Further as the barcode watermark generated follows simple format to represent each digit in PID, so it can be recognized by any normal medical staff visually. Also as the embedded watermark has inherent error detecting capabilities, the extracted watermark can be fully recovered in case of different kinds of attacks.

Hiding the watermarking data in medical image [6, 7] can be done in robust manner so that it prevents the watermark removing unless the quality of the image is greatly reduced. This robust data hiding can be done by embedding watermarking data bits directly in transform domain coefficients like DCT coefficients. Before embedding, high imperceptibility is achieved by adaptively selecting the area of an image in which we can hide more watermark bits compared to remaining DCT blocks by classifying these blocks using k-means clustering method [6, 7].

Most of the researchers focused on embedding whole EPR data in the medical image which may degrade the quality of medical images used for diagnosis in telemedicine applications. Amarit Nambutdee et al. [11] suggested converting patient information data to two-dimensional barcode (ECC200) format image with size of 64x64 bits before embedding the data robustly in DWT-DCT domain. The technique may offer good robustness but suffers from more perceptual distortion as the information to be embedded id large is size. The authors in [12] blind reversible data hiding based on integer wavelet transform, but the scheme may suffer from severe attacks.

In this paper, we propose a method by which we can hide bar-coded binary watermark in HEBs robustly for secure image authentication of medical images at receiver side along with achieving high imperceptibility that is needed for sensitive diagnosis. The rest of paper organized as follows. In section 2, proposed method is explained. Then in section 3, experimental results are given followed by conclusions in section 4.

II. PROPOSED EMBEDDING SCHEME

Proposed scheme consists of following stages as shown in Fig. 1.

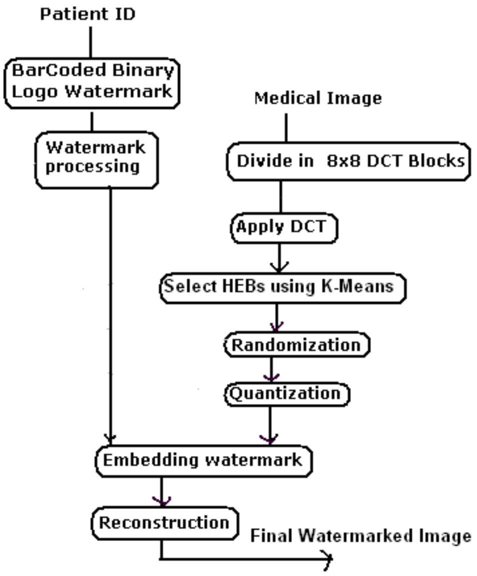
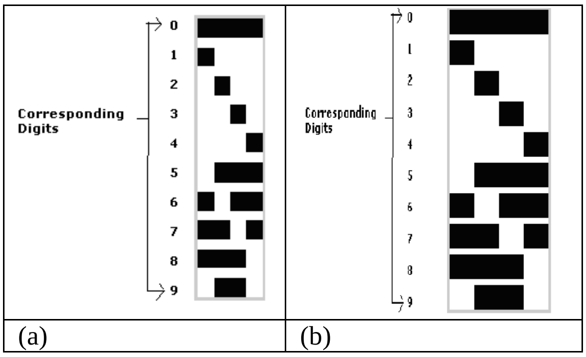


Figure 1: Proposed system

A. Bar-coded Binary Logo Watermark Generation

The 10 digit unique PID (needs only 4 bits to represent each digit so total 40 bits needed) is represented in a human recognizable bar-code logo image format as shown in Fig. 2a and 2b. This format used to represent each digit follows simple pattern so it can be recognized by any normal medical staff visually. A row representing a decimal digit consists of four bars where each bar can be either white or black. After each such row one blank row (1 x 8) is left to improve the visual quality of bar-coded binary logo in case of subjective detection [1]. So for a 10 digit PID, 19 rows (10 rows containing actual PID bits information and remaining 9 blank rows) are needed. For e.g. Fig. 2b shows bar-coded binary logo that is generated in which each bar is 2 x 2 (height x width) pixels in size. Hence each row representing single digit can represent 16 bits of information. Ten such rows containing digit will be of size 2 x 8 and remaining nine rows will be of size 1 x 8. So total number of pixels need to represent 10 digit PID will be 232 in case of 2x2 bar size with interleaved 1x8 blank row size. As it is a binary image (black pixel represented by bit value=0 and white pixel represented by bit value=1 only), the size of watermark logo generated will be 232 bits only.



(a) (b)

Figure 2: Human Recognizable Bar Coded Binary Watermark of sizes (a) 29x8 pixels (b) 49x16 pixels with corresponding digit encodings for given rows

Further to increase robustness and error detection capability of the system and also to achieve more readability, we can increase the dimensions of each bar. For e.g., if each bar is made of 4x4 pixels and each interleaved row is made to have 1x16 size then the total size of the logo will be increased to 784 bits as shown in Fig. 2b. The barcode format used here is human friendly or human recognizable as it follows a simple definite pattern for each digit as given in Table I. As the embedded watermark has inherent error detecting capabilities, the extracted watermark can be fully recovered in case of different kinds of attacks. Before embedding, the generated barcode image can be encrypted using share secret key (Ks) which can be used at the receiver side for extraction process.

1. TABLE I. HUMAN READABLE BARCODE PATTERN

Row Pattern	PID Information Conveyed
All Black	PID Digit is zero
All White	Interleaving Row used for adding visual clarity
Only One Black Bar	Can be PID digit 1 to 4 depending upon location of Black Bar
Only One White Bar	Can be PID digit 5 to 8 depending upon location of White Bar
Two White and Two Black Bars	PID Digit is 9.

B. Watermark Processing Stage

In watermark processing stage, above generated bar-coded binary logo image form can be represented in terms of series of 0's and 1's (bits). Further watermark can be permuted or encrypted to enhance the security of the system.

C. Calculating Energy

Let $X = \{x\{i, j),0 < i < M,0 < j < N\}$ denote the original gray-scale image of size $M \times N$ and $W = \{w\{i, j),0 < i < m,0 < j < m\}$ be the bar-coded binary watermark of size $m \times n$ representing the PID number. Here, $x(i, j) \subseteq \{0,1,...,255\}$ and $w(i, j) \subseteq \{0,1\}$ are the respective pixel intensities of the host image and the watermark image at coordinate (i, j).

First, the host image X is evenly partitioned into $K = \{(M \times N)/(8\times 8)\}$ number of small non-overlapping 8×8 blocks and DCT (Discrete Cosine Transform) is applied to each of these blocks as in (1).

$$Y_k = DCT(X_K) \qquad (1)$$

Where, $0 \le K \le 4096$.
After calculating two dimensional DCT, the energy of each DCT block is calculated as in (2).

$$E_k = \sum_{i=0}^{7}\sum_{j=0}^{7} \| C_{ij} \|^2 - C_{00}^2 \qquad (2)$$

Where, E_k is the energy of k^{th} block and C_{ij} is two dimensional DCT coefficients. DCT coefficient at location $(i = j = 0)$ is neither used for calculation of energy nor for embedding as it degrades the quality of entire block heavily.

D. K-Means clustering

K-Means clustering is a method of cluster analysis which aims to partition n observations into k clusters in which each observation belongs to the cluster with the nearest mean. Given a set of observations $(x_1, x_2,..., x_n)$ where each observation is a d-dimensional real vector, K-Means clustering aims to partition the n observations into k different sets $S = \{s_1, s_2,..., s_k\}$ so as to minimize the within-cluster sum of squares as in (3).

$$\arg\min_{(S)} \sum_{i=1}^{k} \sum_{x_j \in S_i} \| x_j - \mu_i \|^2 \qquad (3)$$

where μ_i μ_{i} is the mean of points in s_i.

The energies of above DCT blocks i.e. $E_K = \{E_0, E_1,..., E_{4096}\}$ are given as input to K-Means algorithm which classifies DCT blocks into two different clusters one having more energy called HEBs and other having less energy called LEBs according to their energy values. HEBs can be used to embed more watermark bits with minimal distortion [7] compared to remaining blocks. Auto selection of HEB blocks is provided by K-Means algorithm rather than the manual selection used in our previous algorithm [8], where choice of energy threshold factor depends on empirical results.

E. Randomization and Quantization

Security of algorithm can be increased by randomly selecting the DCT blocks as shown in Fig. 1. The randomly selected blocks are then quantized for the given value of QF (Quality Factor). After the process of quantization the non-zero predefined DCT coefficients are considered for embedding the watermark information [10]. If the block selected is marked as HEB block, then only four bits of watermark information is embedded in predefined DCT locations in that block. Quantization gives robustness against natural JPEG compression attacks.

E. Embedding and Reconstruction

The watermarking is carried out by suitably modifying the DCT coefficients at predefined locations of the HEB blocks after the process of quantization in order to achieve blind watermarking. In general, the watermark is embedded into middle frequency coefficients of DCT blocks that can provide a better tradeoff between the robustness and imperceptibility According to logical value of a bit to be embedded the rounded value of DCT coefficient gets modulated. If the bit is logically 'zero', the coefficient is rounded to 'even' number, otherwise to 'odd' number. In order to have blind watermark detection at receiver side, mid frequency DCT coefficient at location $(1,2)$ from each DCT 8x8 block is used to convey the information regarding the distinguish between HEBs from LEBs. If it is odd then the block is HEB and contains actual watermark information bits. The final stage of the embedding process is the reconstruction of a watermarked image. This is achieved by IDCT (Inverse Discrete Cosine Transform) and combining all 8×8 image blocks as in (4).

$$X'_k = IDCT(Y'_K) \qquad (4)$$

Fig. 1 shows all the steps of the proposed embedding scheme. The reconstructed medical image is called as watermarked image. The PSNR of this image with respect to original medical image is calculated and compared with expected value of the PSNR. The experimentation shows that after embedding the watermarking information, the Stego-images gives PSNR value more than 40dB.

F. *Watermark Detection*

The extraction algorithm consists of all the image processing steps that are carried out at the time of embedding the DCT blocks i.e. first calculate DCT on each 8×8 non-overlapping watermarked image blocks and then identify HEB Blocks according to the value of DCT coefficient $(1,2)$ of each block. Randomize and quantize HEBs and extract watermark information from the predefined DCT coefficient values. Once all the bits are extracted the bar-coded logo (watermark information) can be reconstructed and unique PID can be retrieved in order to authenticate corresponding medical image. For each 4×4 block of retrieved binary bar-coded logo image, if number of black pixels are greater than some threshold then it is considered as black bar which represents $BitValue = 1$[1]. Similarly if number of white pixels are greater than some threshold then it is considered as white bar which represents $BitValue = 0$. After scanning each row, one white row should be left as it represents blank row. So from each row we get one digit of PID. This retrieved PID can be used further to retrieve complete patient data from central database. Objective detection provides automatic and accurate verification. But it may fail to detect PID, when some unintentional modifications like JPEG compression, brightness change etc. applied to watermarked image. If this objective watermark detection fails then we can still retrieve PID using subjective detection, as each row contains one digit. e.g. if first row contains one black bar followed by three white bars that means bits embedded='1000' which represents most significant digit (MSB) digit in 10 digit PID number.

III. EXPERIMENTAL RESULTS

In the experiments that we conducted we used four different types of standard grayscale radiological medical image files in .bmp format as shown in Fig. 3. The size of the original images is 512x512 pixel gray scale image whereas the size of the watermark logo is 29x8 pixels.

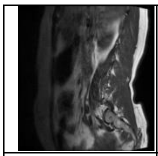
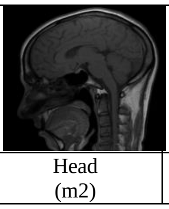
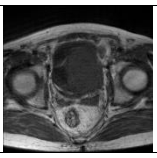
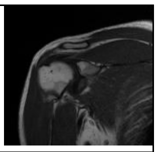
			
L-Spine (m1)	Head (m2)	Abdomen (m3)	Shoulder (m4)

Figure 3: Original Images used for watermarking

The original bar-coded binary watermark logo used in the experiments is shown in Fig. 4, when 10 digit PID= "6847518539" is converted into bar-coded binary watermark image.

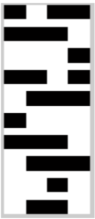


Figure 4: Original bar-coded binary watermark logo

3.1. Perceptual Transparency

Various sets of experimentation are carried out to see the effect of watermark barcode image size and QF on PSNR. As watermark barcode size or QF increases PSNR decreases as shown in Fig. 5.

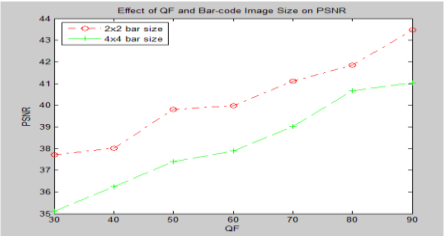


Figure 5: Effect of QF and Bar Size on PSNR

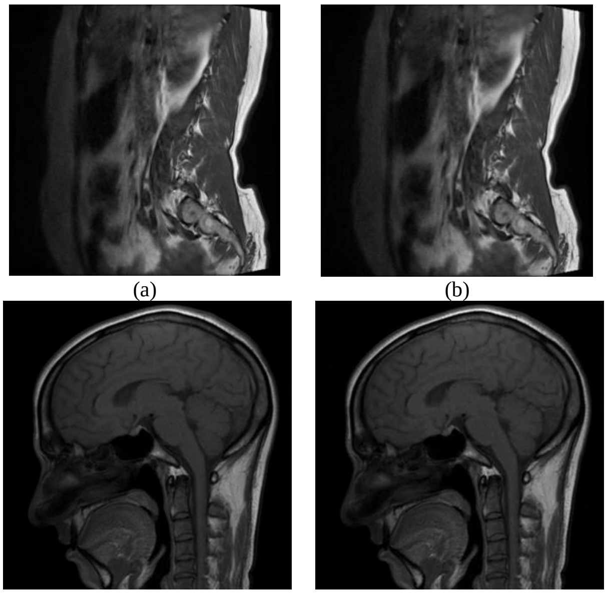

(a) (b) (c) (d)

Figure 6: 'L-Spine' Image: (a) Original (b) Watermarked and 'Head' Image: (c) Original (d) Watermarked

Fig. 6(a) and Fig. 6(b) shows original (Cover) and watermarked 512 x 512 'L-Spine' images while Fig. 6(c) and Fig. 6(d) shows original (Cover) and watermarked 512 x 512 'Head' images respectively. The locations chosen per HEB blocks are at (2,2), (3,0), (0,3) and (0,2) to embed watermark with 'QF =70'. If I(i, j) is an original medical image and I'(i, j) is watermarked medical image then, the PSNR observed for the watermarked image is 45.61dB and is calculated as in (5).

$$PSNR = 10\log_{10}(255^2 / MSE) \qquad (5)$$

where MSE= Mean Square Error given as in (6).

$$MSE = 1/(MxN)\left(\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[I(i,j) - I'(i,j)]^2\right) \qquad (6)$$

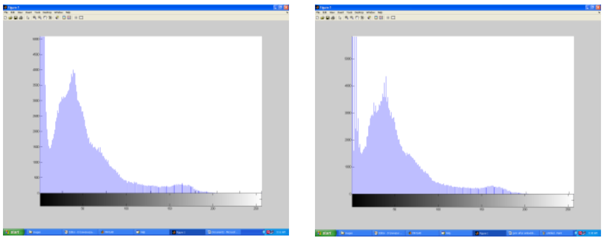
Four different images 'L-Spine (m1)', 'MRI head (m2)', 'Abdomen (m3)' and 'Shoulder (m4)' are observed after watermarking. The resultant watermarked images are observed for two methods – fixed DCT coefficient method where embedding the watermark information done in all DCT blocks and second method where embedding watermark bits done only in HEB blocks suggested by K-Means leaving LEB blocks intact. PSNR of the resultant watermarked images are as shown in Table II.

2. TABLE II. PSNR COMPARISON

Medical Images under Test	PSNR (dB) Fixed DCT coefficient method	PSNR (dB) DCT with K-Means
L-Spine (m1)	39.51	40.55
MRI head (m2)	41.42	42.60
Abdomen (m3)	39.38	41.82
Shoulder (m4)	40.63	42.03

A. Histogram variation in original and stego medical images

Fig. 7 shows the effect of embedding on histogram of both L-Spine and Head medical images.


(a) (b)

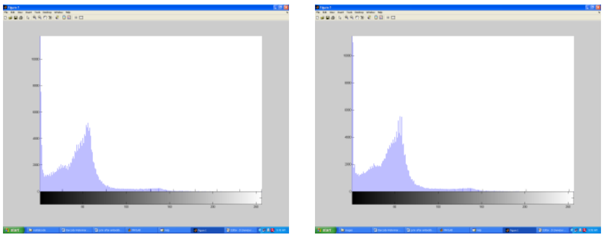

(c) (d)

Figure 7. Effect of embedding on histogram of 'L-spine' image (a) Original (b) Stego and 'Head' image (c) Original (d) Stego

B. HEB and LEB Region

According to value of energies of DCT blocks Fig. 8 shows separation of corresponding HEB Blocks i.e. region of images where watermark information is embedded leaving LEBs (shown in black color) blocks intact.

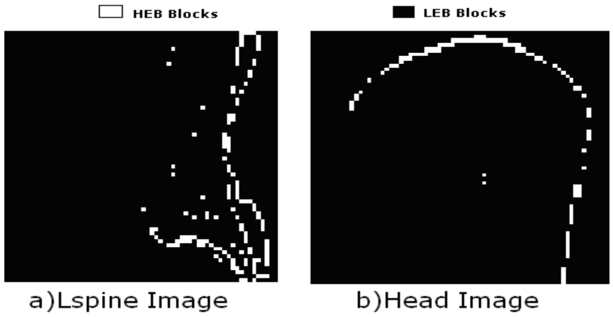


Figure 8: HEB and LEB Block Separation

C. Robustness test

Along with PSNR the Stego-images are also tested against different types of attacks on original images. The NC (Normalized Correlation) between the original transmitted watermark and the watermark extracted from the image used to provide objective measure and calculated as in (7).

$$NC = \sum_{i=0}^{m}\sum_{j=0}^{n} W(i,j)W'(i,j) / \left(\sum\sum |W(i,j)|^2\right) \quad (7)$$

where W(i, j) is an original watermark and W'(i, j) is the extracted watermark.

The watermarked image is subjected to several standard image processing attacks including filtering (median filter with size 5x9), sharpening and blurring. Fig. 9 shows the original cover medical image and corresponding extracted watermark when 10 digit PID= "6847518539" is converted into bar-coded binary watermark image.

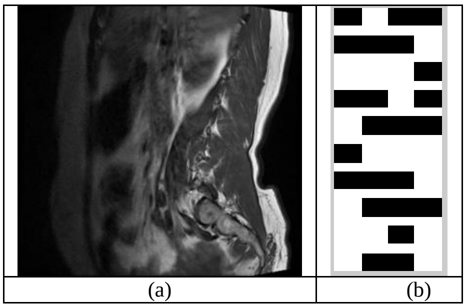
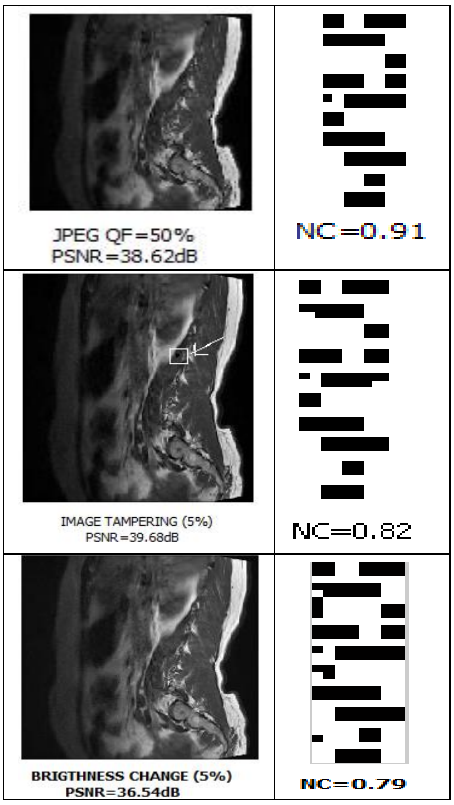


Figure 9: (a) original Medical Cover Image and (b)Extracted watermark when no attack performed

Fig. 10 shows attacked stego images and corresponding extracted watermark images and Table III shows reduction in PSNR along with corresponding values of NC against different attacks. These attacks were carried out on 512 x 512 watermarked 'L-spine' image with 'QF = 70'. The proposed system is found to be robust and gives high correlation of original watermark image and extracted watermark against JPEG compression attack, image tampering attack, image manipulation attack and change in contrast value.



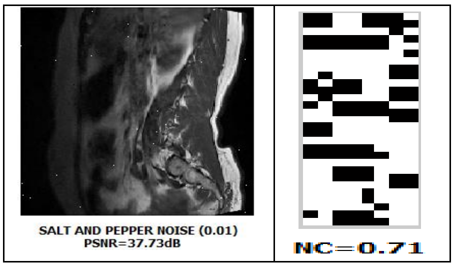


Figure 10: (a) Attacked Medical Image and (b) Bar-coded watermark extracted after attack

The block of extracted watermark gives higher normalized correlation with the original bar-coded watermark block compared to algorithm [8] as shown in Table III. Compared to previous work [8] based on energy threshold technique where energy threshold factor should be decided empirically, proposed scheme is observed to provide the similarity metric NC for all these attacks above 0.7 before correction and almost one after error detection and correction so as to retrieve PID accurately. This shows that the above attacks cannot remove the watermark easily.

TABLE III. NORMALIZED CORRELATION (NC) FOR VARIOUS ATTACKS

Attacks Performed	**Energy Threshold Scheme with Threshold Factor=2.0**		**Proposed Scheme with K-Means**	
	PSNR	***NC (%)***	***PSNR***	***NC (%)***
No attack	42.10	0.83	42.11	1.00
JPEG (QF=50)	38.62	0.70	38.62	0.91
Image Tampering	39.65	0.72	39.68	0.82
Change Brightness	36.54	0.68	36.53	0.79
Median filter size 5x9	38.33	0.73	38.33	0.85
Salt pepper noise	37.71	0.66	37.73	0.71
Sharpening	37.59	0.61	37.59	0.73
Blurring	36.87	0.67	36.88	0.75

IV. CONCLUSIONS

In this paper, we had presented a visually undetectable, blind robust human readable barcode watermarking scheme that allows both objective watermark detection using correlation as well as subjective watermark detection using visual inspection. K-Means algorithm is used to classify the blocks according to their energy values. This adaptive auto selection of blocks for embedding watermark bits using K-Means clustering algorithm increases imperceptibility along with improved normalized correlation compared to energy threshold scheme. Using JPEG quantization reduces the possibility of loss of watermark information drastically but as QF increases, the number of valid coefficients gets reduced which in turn reduces the data hiding capacity. Due to inherent capabilities of error detection and correction of bar-coded watermark logo image, PID can be recovered safely. Effective use of randomization and quantization of DCT blocks while embedding enhances the robustness of the scheme against various attacks like JPEG compression, image tampering and image manipulation. Also as the barcode format used here follows simple definite pattern such that it can be recognized by any medical staff visually in order to determine the corresponding PID number.

ACKNOWLEDGMENT

I thank Dr. Sravan Tungenwar, for providing medical image dataset required for our experimentation. I also thank Defence Institute of Advanced Technology, Pune for providing excellent research facilities to carry out this research work.

REFERENCES

[1] Vidyasagar potdar, Song han, Elizabeth Chang and Chen Wu., “Subjective and objective watermark detection using a novel approach-Bar-code watermarking”, In the proceedings of International conference on Computational intelligence and security, 2006, pp. 1203–1206.

[2] B. Planitz, and A. Maeder, “Medical Image Watermarking: A Study on Image Degradation”, In the proceedings of Australian Pattern Recognition Society Workshop on Digital Image Computing, 2005, Brisbane, Australia.

[3] Zhicheng Ni, Yun Q. Shi, Nirwan Ansari, and Wei Su., “Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication”, IEEE Transactions on circuits and systems for video technology, 2008, Vol. 18, No. 4, pp. 497-509.

[4] Giakoumaki, S. Pavlopoulos, and D. Koutsouris, “Multiple Image Watermarking Applied to Health Information Management”, IEEE Transactions on Information Technology in Biomedicine, 2006, vol.10.4, pp. 722–732.

[5] K. A. Navas, S. Archana Thampy, and M. Sasikumar, “EPR Hiding in medical images for telemedicine”, International Journal of Biomedical Sciences, 2008, Volume 3.1, pp. 44– 47.

[6] Kaushal Solanki, Noah Jacobsen, Upamanyu Madhow, B.S.Manjunath and Sivkumar Chandrashekhar, “Robust Image-Adaptive Data hiding using Erasure and Error Correction”, IEEE Transactions on image processing, 2004, Volume 13, pp. 1627–1639.

[7] Suresh N. Mali, and Rajesh M. Jalnekar, “Imperceptible and Robust Data Hiding using Steganography Against Image Manipulation”, International Journal of Emerging Technologies and Applications in Engineering, Technology and Sciences, 2008, pp. 84–91.

[8] Sunita V. Dhavale, and Suresh N. Mali, “High Capacity Secured Adaptive EPR Data Hiding with Integrity Checking Using CDCS”, International Journal of Computational Science, 2009, Vol. 3, No.6, pp. 657-672.

[9] Neil F. Johnson, and S. Jajodia “Exploring Steganography. Seeing the Unseen”, IEEE Computer, 1998, vol. 3, No. 1.2, pp. 26 – 34.

[10] Min. Wu, “Joint Security and Robustness Enhancement for Quantization Embedding”, IEEE Transactions, 2003, pp. 483–486.

[11] Amarit Nambutdee, and Surapan Airphaiboon, “Medical image encryption based on DCT-DWT domain combining 2D-DataMatrix Barcode”, In the proceedings of 8th International Conference on Biomedical Engineering International Conference (BMEiCON), 25-27 Nov. 2015, Pattaya, IEEE, pp. 1–5.

[12] K. A. Navas, S. Archana Thampy, and M. Sasikumar, “EPR Hiding in Medical Images for Telemedicine”, World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol:2, No:2, 2008, pp. 223-226.