

E2-Invisible Watermarking for Protecting Intellectual Rights of Medical Images and Records

Kavitha K. J.¹

Asst. Prof., Jain Institute of Technology, Davangere &
Research Scholar, CSE Dept, Sathyabama University,
Chennai, India

Dr. B. Priestly Shan²

Principal, Eranad Knowledge City-Technical Campus,
Manjeri, Kerala, India

Abstract—In today's digital era, practice of telemedicine has become common which involves the transmission of medical images and Myhealthrecord (MHR) for higher diagnosis in case of emergency and maintaining integrity, robustness, authentication and confidentiality of such patient's data becomes necessary. Many works has shown that the digital watermarking is one of the solutions but simultaneously, it is known that no complete algorithm is available to fulfil all the requirements of a field. Till the watermarking technique becomes robust, encryption technique can be considered as one of the best solution for protecting the data. Encoding is used for transforming the information in to another form and in the proposed work of digital watermarking (DWM); encoding is combined with encryption and DWM to enhance the protection of data by maintaining the above said constraints. In this paper, DWM for medical images is implemented by joint combination of spatial and frequency domain technique Singular value decomposition-Integer wavelet transform (SVD-IWT) respectively, 64-bit Rivest-Shamir-Adleman (RSA) crypto-technique and new encoding procedure. To avoid the degradation of the medical image which is very essential in the medical field, data payload should be less and is achieved by the use of quick response (QR) code which consumes less space for large information. Finally the proposed system is compared with other traditional methods and also evaluated against various image processing and geometric attacks.

Keywords—Myhealthrecord; SVD; IWT; RSA; QR code; encoding

I. INTRODUCTION

All real time signals are analogous in nature which are easily perceptible and heard by human beings. But in order to process, transmit and receive over the network, these signals should be in digital form and such real time signals are widely used in many of the applications; one of the main applications is in the field of health care system which strictly prohibits any modifications in the information. But any digitally converted data is reversible in nature and in turn leads to many illegal and fraud activities. In such cases, digital watermarking (DWM) system plays a major role for ensuring security, authenticity and confidentiality. The DWM is implemented in two ways: spatial and transform domain [3] [9]; the transform domain is more robust compared to spatial domain but does not provide complete contribution towards the security of the information.

The DWM technique does not avoid the fraud cases but however it can help in preventing and reducing illegal use of the data. So, until the DWM system becomes robust enough to prevent the removal of watermark content from it, the research in this field continues.

Most commonly used and efficient techniques are; Spatial LSB and transform IWT techniques. The SVD technique embeds the WM in the LSB of pixels but does not create serious distortion but is less robust. In DWT, the watermark is embedded in floating point coefficients so that any truncations of the floating point values of the pixels that should be integers may lead to the loss of the watermark information which may in turn lead to the failure of the system. In order to avoid the loss of information IWT technique involves only integer so that there is no loss of information. Thus one of the alternate to increase the robustness of DWM is to combine the positive features of spatial and frequency domain technique [12]. Although the techniques are combined, it cannot avoid the removal and identification of watermark. Therefore the limitation of DWM can be clubbed with encryption [6] and encoding technology to secure the confidential data in the field of health care systems.

Encoding is the process of converting one form of information to another form and this property of encoding is used to hide the original data from the fraud. In this paper, the watermark information is encoded with the help of generation of large value of prime numbers and is done with new proposed algorithm and later encoded message is encrypted using 64-bit RSA crypto algorithm (only for simulation purpose and we can use 1024-bit RSA also). The process of encoding followed by the encryption ensures double blinded security [2] to the information.

Prime numbers are used in both encoding and encryption process and it is very difficult for anyone to predict the large prime factorized value and this property of prime numbers adds the benefit in improving the security.

In the medical field modification of the data is not entertained as it may lead to inappropriate decision even by the specialized doctors and to avoid such cases, data payload should be less and to achieve this quick response code (QR) [7] [15] is used in the proposed watermarking system.

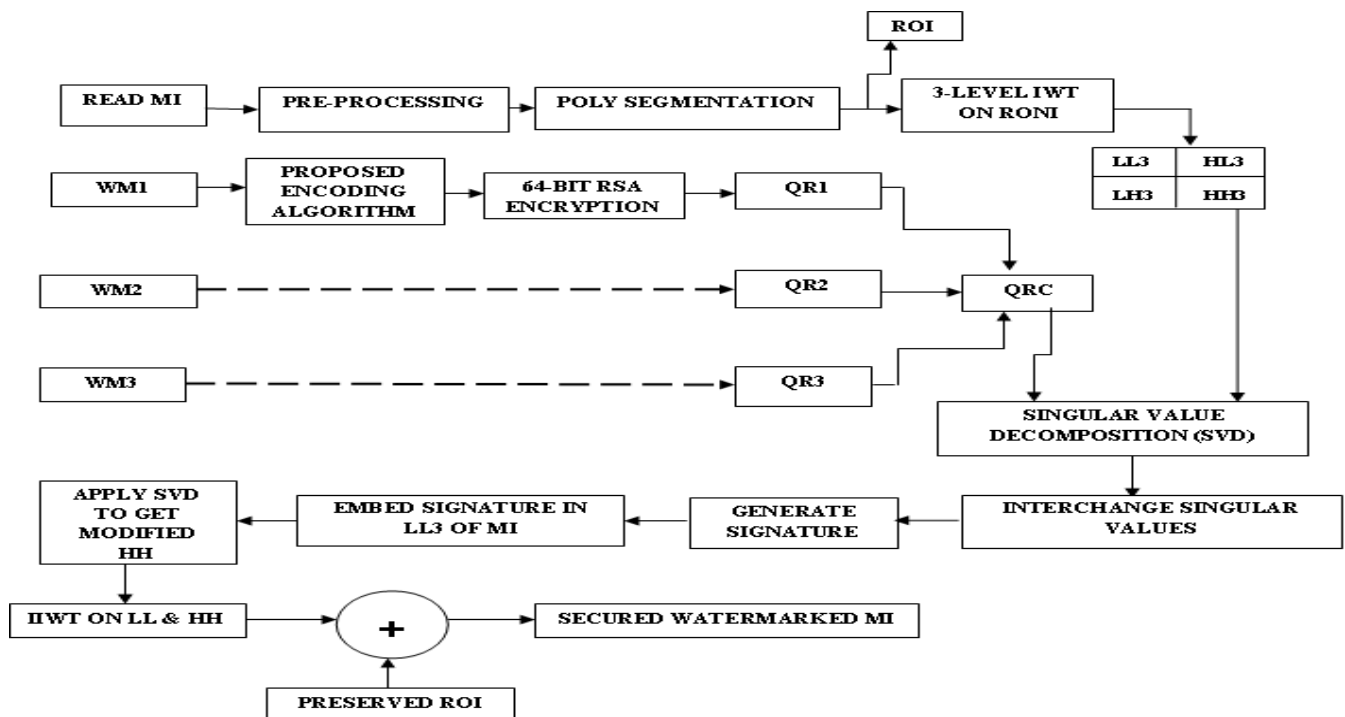


Fig. 1. Proposed Block Diagram of WM Embedding Process.

II. PROPOSED ALGORITHM

Here a novel Encoding-Encryption (E2)-based DWM embedding procedure is proposed for MI and is shown in the figure 1. In this work, three different watermarks are used; patient information, patient ID (E-aadhar) and hospital logo. The patient information is encoded using the proposed encoding algorithm followed by 64-bit RSA encryption algorithm. The same operation can be done with other watermark information also but for simplicity here these steps are performed only with the patient details.

A. Pre-processing Steps at the Scanned MI:

Step1: Read the scanned MI from the database (Cover Image).

Step2: In pre-processing, color image is converted to gray image. The conversion is done as gray scale image is represented by 8-bit value ranging from 0-255. With contrast to RGB MI which is represented by 24-bit, the gray image processing has many advantages such as: complexity of the code is less; speed of computation is very high as it processes only with one channel elements; signal to noise ratio is high compared with 3-channel colour image;

Step3: After the conversion, the image is subjected to polygon based segmentation to separate region of interest (ROI) region and region of non-interest (RONI) region as shown below. Segmentation is necessary in the case of MI so as to avoid the degradation of the diagnosis part. The diagnosis part is considered as ROI and the rest is RONI. Most of the radiologist use polygon based segmentation because of its easiness i.e. it just involves selecting four points on the positive and negative axis as shown in figure2:

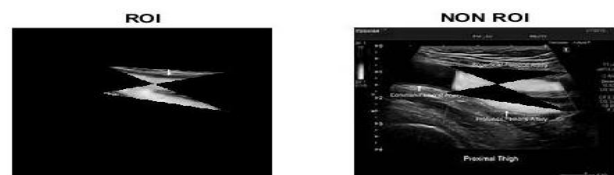


Fig. 2. Polygon Segmentation To Separate ROI & RONI before Embedding Process.

After separating ROI region, the watermark can be embedded in to the RONI region without distorting the useful information.

Step4: This step is explained later in the section of watermark embedding process.

B. Steps Performed at the Watermark:

Step1: Read 3 different watermarks: Patient details (txt, doc, excel), Patient ID (E-aadhar) and hospital logo.

Step2: Apply the proposed encoding algorithm to get encoded message in terms of prime numbers. The encoding algorithm is described below:

- 1) Read the first watermark i.e. patient detail file K from the database.
- 2) Read the total length of the characters M and assign it to another variable N for future use.
- 3) Read each character from the file.
- 4) Generate a random prime number KL.
- 5) Using the above value, once again generate random prime numbers for each character.
- 6) Store the last prime number in a variable key.

- 7) Divide the entire length in to half.
- 8) Apply the algorithm as described below

$$\begin{aligned} & \text{for } i = 1 \text{ to } M/2 \\ \text{enc}(i) &= (p(i) + p(N) + K(i)) \oplus \text{key} \\ \text{enc}(N) &= (p(i) - p(N) + K(N)) \ominus \text{key} \\ & N = N - 1 \end{aligned}$$

Where

$p(i)$ → prime number of i th character

$p(N)$ → prime number of N th character

Repeat the above process for all characters.

In broad way encoding is considered as a method of transforming the original information in to another form which is easily not understood by common persons. In the encoding procedure mentioned above, the prime numbers are used in the process of addition; subtraction, modulo-2 additions and subtraction are used.

Step3: Apply 64-bit RSA encryption to the encoded message. The RSA encryption technique involves the generation of private key, public key and modulus. The public key can be shared among the doctors while retaining the private key with the patient to maintain confidentiality, authenticity and security.

The procedure for generating the 64-bit key is described below:

- a) The encoded message is converted to 64-bit integer data type.
- b) Generate the key pair: modulus, public and private key
 - i. Select two large prime numbers p & q .
 - ii. Compute modulus $m = p \times q$
 - iii. Calculate $k = (p - 1) \times (q - 1)$
 - iv. An integer selection between the range $1 < e < n$ and is used as a public key 'e'.
 - v. Private key 'd' is generated using integer e and two prime numbers p & q using extended Euclidian algorithm (used to obtain gcd-last non zero remainder).
 - vi. Later encryption is performed using modulus, public key 'e' and the message as:

$$\begin{aligned} & \text{initialize Encrypted message} = 1 \\ & \text{temppublic} = 0 \\ & \text{temppublic} = \text{temppublic} + 1 \\ \text{Encrypted message} \\ &= \text{mod}((\text{individual character of the message} \\ & \times \text{Encrypted message}), k) \\ & \text{if } (\text{temppublic}) = e \\ & \text{stop encryption} \end{aligned}$$

Step4: QR code is generated using zxing library function for encrypted message to reduce the data payload. QR code is widely used nowadays because of its less space consumption to that of bar code or any other conventional symbol, isotropic property, capacity to hold 7092 characters of data which may

consist of numbers, symbols, text, control codes etc both horizontally and vertically and rather than this even if it is damaged it is possible to recover the data from 30 to 35% of the damaged data [4] [5].

Step5: The same procedure may be done for other watermarks also with slight modifications. But in this paper, the steps are performed only for patient details. Rather than this, QR code is generated for other two watermarks. The sizes of patient ID (E-Aadhar) of size 40.4KB of dimension 252×365 , Hospital Logo of size 3.57 KB with dimension 47×43 and PHR of size 12.47 KB with dimension 268×218 are used.

Step6: The generated three different QR code watermarks are concatenated with three different colours R, G and B to differentiate each other.

$$\text{QRC} = \text{cat}(3, R, G, B)$$

Step7: The concatenated QR code is applied with SVD.

C. Watermark Embedding Process

The procedure for embedding the QR watermark is described below: The process involves the use of frequency domain IWT technique and spatial domain technique SVD [10]. The RONI obtained after segmentation is subjected to 3-level Integer Wavelet Transform (IWT) which is usually considered as Reversible Lifting Wavelet Transform (RLWT). Nowadays IWT is replacing Discrete Wavelet Transform (DWT) as it eliminates the information loss in the fractional part of the data during watermark [1] embedding process as it involves integer to integer transform mapping that does not allow the information loss during the forward and reverse process. The deeper level decomposition is considered, as the 1-level decomposition does not contain much information while the subsequent levels contain more information and less noise. Embedding the watermark in such deeper levels provides more robustness to the system.

a) Apply 3-level IWT to the RONI region of MI which results in four frequency bands as low-low (ll), low-high (lh), high-low (hl) and high-high (hh) followed by SVD operation.

b) Since the high frequency component is less informative, modifying the data in this part does not affect, hence the hh part of MI is used to generate the signature that is to be embedded in ll part of MI. The ll part is chosen for embedding as we know that, the low frequency part is more informative and hiding the data in such part is not easily traceable and thus we can evaluate the robustness of the system.

The signature generation involves the following steps [8]:

- i. Apply SVD to the higher frequency band hh of MI and it gives u_i , s_i and v_i .
- ii. Apply SVD to the QR code watermark and it gives u_w , s_w and v_w .
- iii. Singular component of MI and WM are exchanged to get modified hh band of the MI.
- iv. The remaining u_w and v_w components of WM are used along with a random constant key to generate the signature.

v. To generate signature, initially a threshold value is fixed either to 0 or 1 based on the median values of sum of u and v components and reshaped to 1×256 column elements.

vi. Perform XOR operation on the above elements to get 1×512 sized element.

vii. Now this is XORed with a random key selected resulting in signature.

c) The generated signature is embedded in the low frequency band II of MI.

i. While embedding process, IWT is applied at 3-level decomposition.

ii. The ll3 and hh3 of the above result is reshaped to 1×256 and both are concatenated to get 1×512 sized component.

iii. After concatenation, separate the negative and positive decimals and store the negative values for reconstruction purpose in the later stage.

iv. Again separate the integer and fractional part in the positive decimal part and convert integer part to 32-bit binary.

v. Chose n^{th} bit for embedding signature, in this 20^{th} bit is replaced by the signature.

vi. After performing embedding operation, convert binary to decimal once again and add the fractional part and negative indices stored.

d) Now apply SVD to the modified hh band (which holds singular value of WM) and perform the inverse IWT to this and the result obtained in step c.

e) Combine the above result with preserved ROI to get watermarked MI.

D. Watermark Extraction Process

The watermarked image may be either stored in the database or transmitted over the network, if required for higher diagnosis. At the recipient side, the received image has to be validated by extracting the embedded watermark and reconstructing the original MI. The watermark extraction and reconstruction of MI is done using watermarked image, watermark and a random key as described below:

1) Read the watermarked image from the database, separate ROI & RONI as shown in figure 3 and then apply 3-level IWT to the RONI part.



Fig. 3. Polygon Segmentation to Separate ROI & RONI before Extraction Process.

2) Apply SVD to the watermark image and generate the signature using the received key.

3) Extract the signature from the watermarked image using u and v components of WM and a key (it can be sent over phone or any other method) using the same process as that of signature embedding and signature is generated using the original WM using the same method as that in the watermark embedding process.

4) The generated signature is matched with the extracted signature to get authentication. If both the signatures are matched, then it proves authentication and allows for the next step of watermark extraction.

5) After successful authentication, SVD is applied to the hh frequency band of watermarked MI and the singular value of hh band is extracted.

6) The watermark is constructed with u_w, v_w components of watermarked MI of step II and result of step V or inverse IWT to get original MI as shown in figure 4.

7) Later the QR code watermark is decatenated.

After the construction of watermark which is in the QR code is decoded using built in zxing qr code decoder to get the encrypted data. This data is decrypted using 64-bit RSA decryption algorithm and to do this at the receiver a modulus value m and a public key e. The decryption procedure is described below:

a) For decryption, it requires encrypted information, private key and modulus.

b) The same process is carried out as that of encryption except only with respect to private exponent.

Now the decrypted data is passed through the decoding stage which is exactly opposite to that of encoding stage at the transmitter to get the patient detail. The decoding procedure is described below:

$$\begin{aligned} & \text{for } i = 1 \text{ to } M/2 \\ K(i) &= (enc(i) \ominus key) - p(i) - p(N) \\ K(N) &= (enc(N) \ominus key) - p(i) + p(N) \\ & N = N - 1 \end{aligned}$$

8) The RONI part of the watermarked image is combined with the ROI which was separated in step I to get the original MI.

The overall process of generating the patient's MHR is shown in figure 5.

The extracted watermark and reconstructed MI are compared with the original watermark and the original MI respectively and evaluated using the quality metric parameters PSNR, MSE and SSIM. Also the system robustness is verified against various attacks like JPEG compression, Median filter, Wiener filter, and Gaussian filter, Image cropping, Image rotation and Image resize [11] [14].

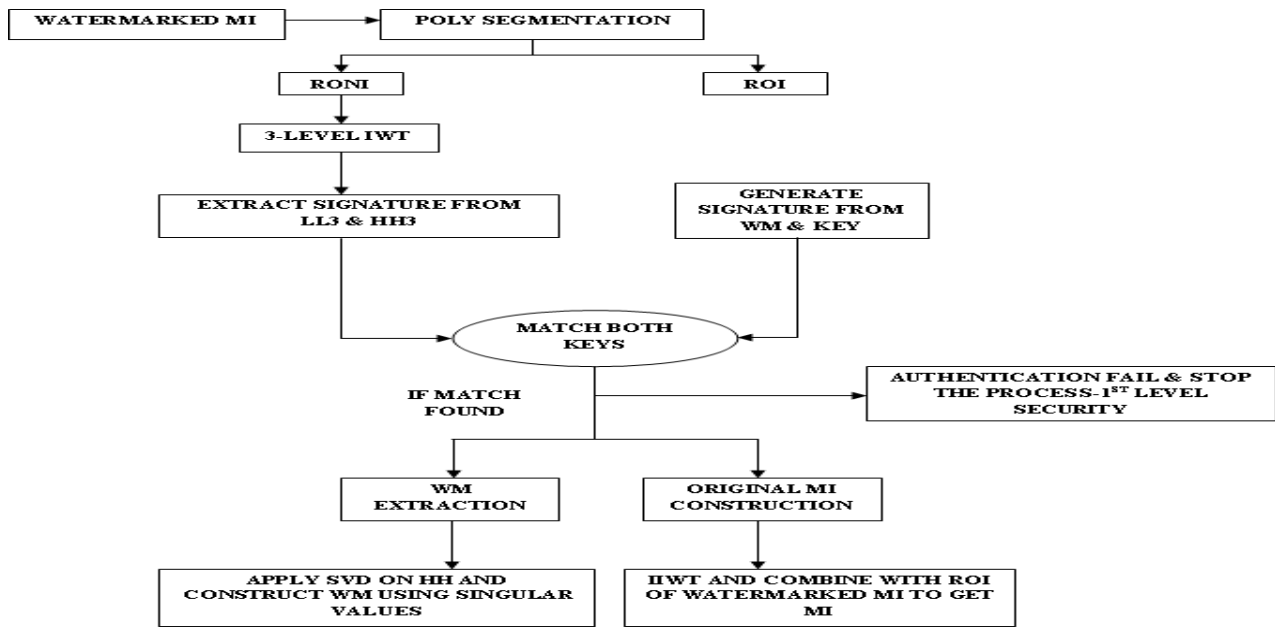


Fig. 4. Block Diagram of Proposed WM Extraction Process.

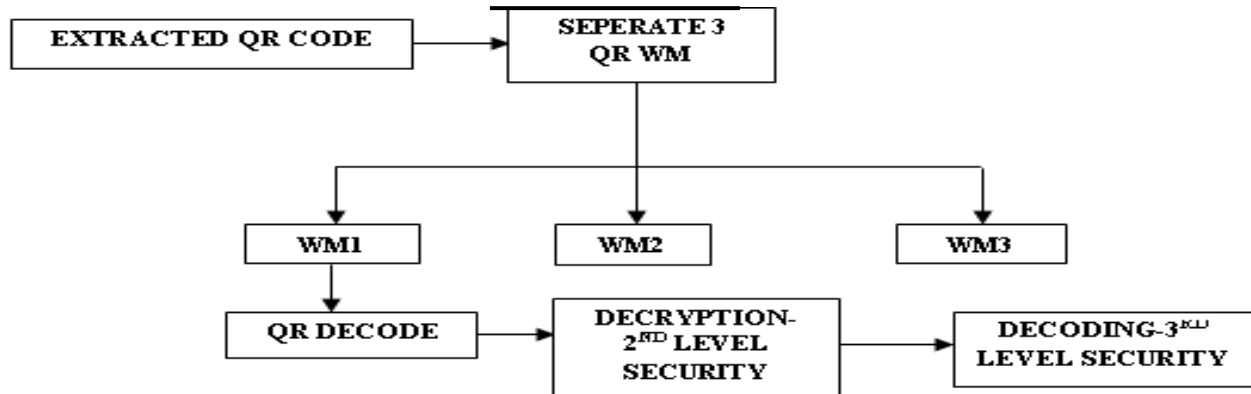


Fig. 5. Block Diagram of Generating the Original Patient Information.

E. Results and Discussion

The proposed algorithm is simulated using Mat lab 2015a. In the proposed work, a combination of spatial domain technique SVD and frequency domain technique IWT together with encoding, encryption and QR code is proposed. The main advantage of SVD is that the singular value of image provides the specifications about the geometry of image such as; left and right singular vectors represents horizontal and vertical details of image whereas the singular values specifies the luminance of the image. And small variations to such vectors will not affect the image quality [13].

On the other hand IWT is used for lossless data compression and also computation speed of IWT is much higher than that of DWT as it does not involve the fractional part. IWT is implemented using the lifting scheme method which consists of 3 steps; split, predict and update. Another main advantage of using IWT is that it is reversible in nature i.e. the image can be reconstructed without any loss as its coefficients are stored without rounding off errors.

Moreover combined use of encoding and encryption doubles the security of the information and QR code can ensemble a bigger data. The US medical images used in the simulation process are collected from the online data base and some of MRI images are collected from SS health care centre.

The result of encoding, QR code generation, encryption and the respective reverse operation are shown in table I and the overall watermark embedding and extraction process is shown in table II. The table III gives the performance evaluation of the proposed system for a single key against other traditional methods.

The table IV & V gives performance evaluation of the system verified for 20 random keys. For evaluation of the system the quality metric parameters PSNR, SSIM, MSE, false acceptance and rejection ratio are considered. The figure 6 shows graph of false acceptance & rejection ratio, decoding correct & wrong information at the receiver side. The table VI gives the evaluation of the system against various image processing & geometric attacks.

TABLE I. RESULTS OF ENCODING, ENCRYPTION AND THE REVERSE PROCESS DURING WM EMBEDDING AND EXTRACTION PROCESSES


<p>Hospital: SS Hitech Health care</p> <p>Doctor In charge: Dr. Sanjay S</p> <p>Name of the Patient: Kavitha K J</p> <p>Date Of Birth: 19/02/1982</p> <p>Age: 36 years</p> <p>Date of Admission: 19/07/2018</p> <p>Patient ID: SS_IP_54786_022018</p> <p>Health Issue: Leg fracture below the ankle</p> <p>Precaution: Rest for 3-weeks</p> <p>a. Patient detail</p>	<p>Encoded message:</p> <p>'201036,138225,243711,121578,41379,109004,71983,97310,77308,130178,94803,95117,112154,30922,40577,110832,127047,179003,138216,133674,198552,141419,41683,240182,163414,86754,114428,157685,78031,162234,150935,226699,112038,44230,220975,88469,190356,93159,134568,156734,169615,77390,190780,18133,89214,227257,180464,116703,105147,127966,57832,176844,78332,227284,222710,183575,221407,41702,100190,169155,43657,118564,79041,165331,139236,121734,110123,208611,139251,95050,223271,78714,90726,156066,121328,5705,113702,184712,132129,131112,154105,149129,152416,-----</p> <p>b. encoded message of (a)</p>
<p>Ciphertext: 1347 1963 301 1963 2989 2969 682 301 2989 84 1347 1347 1325 682 1347 2013 2989 1145 301 301 682 301 1347 301 1325.....</p> <p>c. encrypted message of (b)</p>	 <p>d. QR code of (c)</p>
<p>-Key Pair-</p> <p>Modulus: 4189</p> <p>Public Exponent: 3</p> <p>Private Exponent: 2707</p> <p>Restored storage: 1347 1963 301 1963 2989 2969 682 301 2989 84 1347 1347 1325 682 1347 2013 2989 1145 301 301 682 301</p> <p>e. Decrypted message of (d) after QR decoding</p>	<p>Decoded Message:</p> <p>'201036,138225,243711,121578,41379,109004,71983,97310,77308,130178,94803,95117,112154,30922,40577,110832,127047,179003,138216,133674,198552,141419,41683,240182,163414,86754,114428,157685,78031,162234,150935,226699,112038,44230,220975,88469,190356,93159,134568,156734,169615,77390,190780,18133,89214,227257,180464,116703,105147,127966,57832,176844,78332,227284,222710,183575,221407,41702,100190,169155,43657,118564,79041,165331,139236,121734,110123,208611,139251,95050,223271,78714,90726,156066,121328,5705,113702,184712,132129,131112,154105,149129,152416,148386,179904,79056,98751,92727,216716,25261,89962,214886-----</p> <p>f. Decoded information of (e)</p>
<p>Y= Hospital: SS Hitech Health care</p> <p>Doctor In charge: Dr. Sanjay S</p> <p>Name of the Patient: Kavitha K J</p> <p>Date Of Birth: 19/02/1982</p> <p>Age: 36 years</p> <p>Date of Admission: 19/07/2018</p> <p>Patient ID: SS_IP_54786_022018</p> <p>Health Issue: Leg fracture below the ankle</p> <p>Precaution: Rest for 3-weeks</p> <p>g. Reconstructed message</p>	

TABLE II. RESULTS OF WM EMBEDDING AND EXTRACTION PROCESS

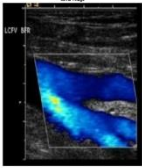

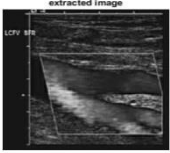
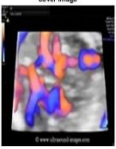
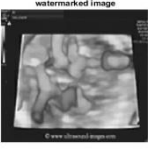
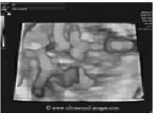
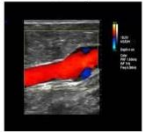


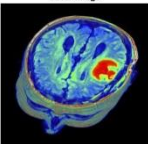
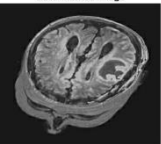
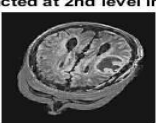





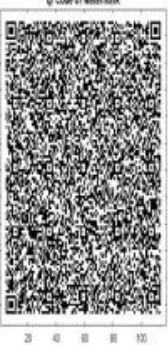
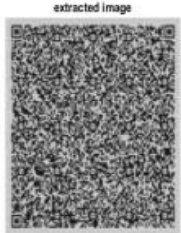
Type of image	Cover Image	Invisible watermark	Reconstructed MI
2-D US			
3-D US			
2-D MRI			
3-D MRI			
WM1, WM2 & WM3	QR watermark	Concatenated watermark	Extracted watermark
 File Edit Format View Help Hospital: SS Hitech Hospital Doctor Incharge: Dr. Sanjay S Patient ID:SS_IP_547896_022018 Name: Kavitha K J DOB:19-02-1982 Age:36 years Date of Admission:02-02-1986 Health Issue: Pain_hand_ankle Severeness:Medium Precaution: Do not hold heavy load 	  		

TABLE III. EVALUATION AND COMPARISON OF THE PROPOSED SYSTEM FOR A SINGLE KEY

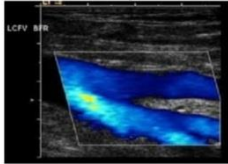
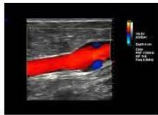

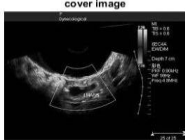
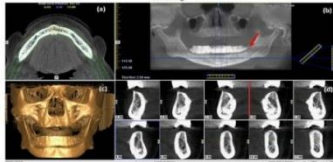
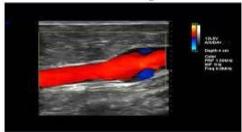
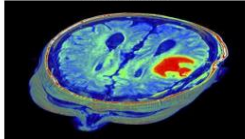
Type of MI	Results of Proposed system with encoding & encryption	IWT-SVD without encoding & encryption	Bit-plane Method	DWT-SVD
	PSNR= 79.117 MSE= 0.0038 NCC= 0.9961 NAE= 0.3549	PSNR= 79.117 MSE= 0.0038 NCC= 0.9961 NAE= 0.3549	PSNR= 49.248110 MSE= 0.8827 NCC= 0.4413 NAE= 0.6315	PSNR= 44.9961 MSE= 2.097 NCC=0.876 2 NAE= 0.9810
	PSNR= 75.1518 MSE= 0.0056 NCC= 0.9890 NAE= 0.3559	PSNR= 75.1518 MSE= 0.0056 NCC= 0.9890 NAE= 0.3559	PSNR= 47.677981 MSE= 1.0576 NCC= 0.6976 NAE= 0.7476	PSNR= 44.8512 MSE=2.145 NCC= 0.8903 NAE= 0.9891
	PSNR= 74.0176 MSE= 0. 0061 NCC= 0.9874 NAE=0.03612	PSNR= 74.0176 MSE= 0. 0061 NCC= 0.9874 NAE=0.03612	PSNR= 48.224884 MSE= 0.9970 NCC= 0.6976 NAE= 0.6945	PSNR= 45.004 MSE= 2.070 NCC= 0.8967 NAE= 0.8612
	PSNR= 77.3791 MSE= 0.00581 NCC= 0.9880 NAE= 0.03653	PSNR= 77.3791 MSE= 0.00581 NCC= 0.9880 NAE= 0.03653	PSNR= 54.8284 MSE= 0.8702 NCC= 0.8676 NAE= 0.7951	PSNR= 45.0682 MSE= 2.040 NCC= 0.899 NAE= 0.8524
	PSNR= 73.613 MSE= 0.0072 NCC= 0.9752 NAE= 0.03721	PSNR= 73.613 MSE= 0.0072 NCC= 0.9752 NAE= 0.03721	PSNR= 55.4684 MSE= 0.8920 NCC= 0.7987 NAE= 0.8211	PSNR= 44.7503 MSE= 2.195 NCC= 0.8941 NAE= 0.7853
	PSNR= 74.613 MSE= 0.00260 NCC= 0.9652 NAE= 0.03721	PSNR= 74.613 MSE= 0.00260 NCC= 0.9652 NAE= 0.03721	PSNR= 52.132 MSE= 0.8672 NCC= 0.7852 NAE= 0.7217	PSNR= 42.113 MSE= 2.7214 NCC= 0.7952 NAE= 0.7291
	PSNR= 72.0173 MSE= 0.0142 NCC= 0.9321 NAE= 0.03721	PSNR= 72.0173 MSE= 0.0142 NCC= 0.9321 NAE= 0.03721	PSNR= 53.161 MSE= 0.7275 NCC= 0.6752 NAE= 0.721	PSNR= 43.263 MSE= 2.6525 NCC= 0.6092 NAE= 0.7721

TABLE IV. SSIM, PSNR AND MSE VALUES FOR 20 SECRET KEYS

Keys	SSIM	PSNR	MSE
1	0.9967	75.004	0.070
2	0.9905	74.949	0.096
3	0.997	78.996	0.074
4	0.9908	77.880	0.130
5	0.9889	76.750	0.195
6	0.9938	79.011	0.066
7	0.9920	80.843	0.148
8	0.9990	81.814	0.162
9	0.9963	77.004	0.070
10	0.9031	82.866	0.137
11	0.9412	81.019	0.063
12	0.9913	79.926	0.108
13	0.9962	78.941	0.100
14	0.9895	77.736	0.202
15	0.9859	80.821	0.159
16	0.9933	79.063	0.040
17	0.9899	82.949	0.097
18	0.9920	78.851	0.145
19	0.9974	79.934	0.104
20	0.9877	80.996	0.074

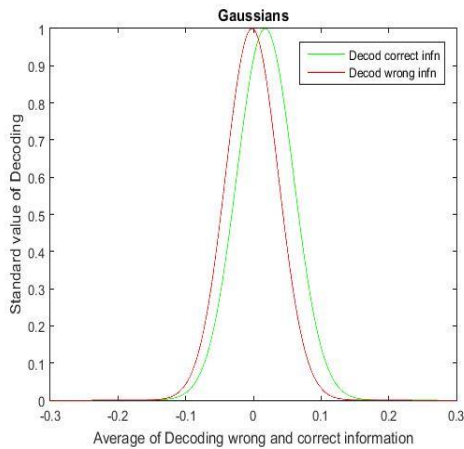
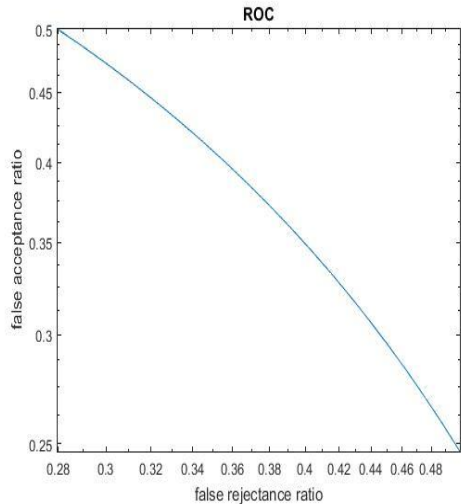


Fig .6. False Acceptance & Rejection, Average of Decoding Wrong And Correct Information.

TABLE V. FALSE POSITIVE AND FALSE NEGATIVE VALUE FOR 20 KEYS

Keys	Pfa	Pfr
1	0.5	0.320
2	0.489	0.329
3	0.478	0.338
4	0.468	0.347
5	0.458	0.356
6	0.447	0.365
7	0.437	0.374
8	0.426	0.384
9	0.416	0.393
10	0.406	0.403
11	0.396	0.412
12	0.385	0.422
13	0.375	0.431
14	0.365	0.441
15	0.356	0.451
16	0.346	0.460
17	0.336	0.470
18	0.327	0.480
19	0.317	0.490
20	0.308	0.5

TABLE VI. EVALUATION OF THE PROPOSED SYSTEM AGAINST VARIOUS ATTACKS

Various attacks	PSNR(db) for Attacked watermarked image & Original watermarked image	
JPEG ATTACK	69.27	
MEDIAN FILTER	Filter size	
	[3 3]	84.7833
	[6 6]	77.5902
	[10 10]	75.514
WEINER FILTER	[3 3]	78.7029
	[6 6]	77.9213
	[10 10]	77.2466
GAUSSIAN FILTER	Q=0.5	91.93
	[3 3]	
	[6 6]	88.997
	[10 10]	78.997
PEPPER & SALT	71.3563	
SHARPEN	72.3563	
ROTATION WITH $\pm 90^\circ$	71.099	

F. Conclusion

In the proposed work, robust blind reversible DWM technique has developed which includes 3-level security. The main idea behind this technique is to protect the original patient's information from third parties. In this methodology, one may not be easily able to identify the information as it ensures three stages of security level viz.; extraction & decoding the information from QR code followed by decryption and decoding processes. Moreover the system shows more robustness against various attacks and the quality of the MI is maintained even for large data payload.

In a single QR code a maximum of 3KB of data may be embedded and hence a new method of storing maximum data and thus reducing the data payload is to be found in future.

REFERENCES

- [1] M. Malonia et.al "Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression technique," *2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, 2016, pp. 1-6.
- [2] C. Zhang, et.al, "Digital Image Watermarking Algorithm with Double Encryption by Arnold Transform and Logistic," *2008 Fourth International Conference on Networked Computing and Advanced Information Management*, Gyeongju, 2008, pp. 329-334.
- [3] C. Su, J. Huang, C. Shih, and Y. Chen, "Reversible and Embedded Watermarking of Medical Images for Telemedicine," pp. 145-150, 2015.
- [4] Kavitha K. J, Shan P., An efficient medical image watermarking technique using integer wavelet transform and quick/fast response codes,(InPress),IJISTA,Inderscience publication.
- [5] J. Chen, W. Chen, and C. Chen, "Identification Recovery Scheme using Quick Response (QR) Code and Watermarking Technique," vol. 596, no. 2, pp. 585-596, 2014.
- [6] C. Engineering and C. Engineering, "a security technique based on watermarking and encryption FOR,"pp. 3-6, 2015.
- [7] Y. Guo, et.al, Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain. *IET Image Processing*, 2017 June, 11(6), pp. 406-415.
- [8] Kavitha K. J, Shan P. B. Joint Digital Water Marking for Medical Images for Improving Security. *Biomed Pharmacol J* 2018;11(2).pp.863-870.
- [9] Maity, et.al, Robust and Blind Spatial Watermarking In Digital Image. *ICVGIP*. 2002.
- [10] Alirezanejad, et.al. Improving the performance of spatial domain image watermarking with high boost filter. *Indian Journal of Science and Technology* ,2014,7(12),pp. 2133.
- [11] Lee, et.al, Analysis of Attacks on Common Watermarking Techniques. IEEE, Electrical and Computer Engineering Department University of British Columbia, Canada V6T1Z4.
- [12] Sarkar, et.al, Digital Watermarking Techniques in Spatial and Frequency Domain. *arXiv preprint arXiv: 1406.2146* (2014).
- [13] Z. Nana, Watermarking algorithm of spatial domain image based on SVD. *2016 International Conference on Audio, Language and Image Processing (ICALIP)*, Shanghai, 2016, pp. 361-365.
- [14] Chun-Shien et.al, Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection. *IEEE Transactions on Multimedia*, 2006 August, 8(4), pp. 668-685.
- [15] K. J. Kavitha and B. P. Shan, Implementation of DWM for medical images using IWT and QR code as a watermark, 2017 Conference on Emerging Devices and Smart Systems (ICEDSS),doi={ 10.1109/ICEDSS.2017.8073698},pp.252-255.

AUTHOR'S PROFILE



Kavitha KJ, presently working as Asst Prof in Electronics & Communication Engineering Department in Jain Institute of Technology, Davangere, Karnataka. She has a teaching experience of total 14 years. She got her Bachelor of Engineering in Electronics & Communication Engineering from Tontadarya college of Engineering, Gadag in the year 2003, and Master of Technology in Computer Science and Engineering from Bapuji Institute of Engineering & Technology, Davangere in the year 2009 from VTU, Karnataka. She is currently pursuing her Philosophy of Doctorate in the field of Medical Images using Image processing Technique using Mat lab in Sathyabama University, Chennai, Tamilnadu.



Dr. Priestly B Shan, presently working as Principal,Eranad Knowledge City-Technical Campus, Manjeri, Kerala. He also worked as a Dean in Royal College of Engineering,India, as a Professor in AmalJyothi College of Engineering, Kottayam, India,StJosephs College of Engineering, India and Muthayammal Engineering College. He got his Master degree fom Anna University,India and Philosophy of Doctorate in the field of Medical Imaging from Anna University in the year 2010,Chennai,tamilanadu.He has also done Msc Applied Psychology, Psychology from Bharathidasan University. He was IEEE member and Life Member in ISTE, IETE and IACSIT. He has also accomplished a research project on 4D ultra sound.