# **An Efficient Method for Digital Image** Watermarking Based on PN Sequences

Shivani Garg, Mtech Student Computer Science and Engineering BBSBEC Fatehgarh Sahib, India shivani.3.garg@gmail.com

Ranjit Singh, Assistant Professor Computer Science and Engineering BBSBEC Fatehgarh Sahib, India jitbhatthal@yahoo.com

Abstract—In the recent times, the rapid and extensive growth in Internet technology is creating a pressing need to develop several newer techniques to protect copyright, ownership, authentication and content integrity of digital media. A potential solution to this kind of problem is digital watermarking. Numerous methods have been presented in the literature and several watermarking software packages have been developed. Still robustness and security of watermark against a variety of attacks is one of the most important issues to be solved. In this paper, Discrete wavelet transform is used to provide robustness and spread spectrum technique is used to provide security. The results are evaluated by applying number of attacks.

## Keywords- Haar Wavelet, M-sequences, Gold Sequences, Kasami sequences, PSNR, NCC I

II.

INTRODUCTION

With the revolution of information technology and Wide Area Networking, data has become less and less private where the access of media as well as the attempts to change and manipulate the contents of media data has become a common case. Digital Watermarking is an important issue in the field of multimedia security protection[7]. Digital Watermarking is a technique that proffers a means to verify authenticity and to guard digital images from illegal copying and manipulation. The procedure of embedding data into a multimedia element like image, audio or video is referred to as watermarking. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low-energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format. As the robustness and security, both are challenging areas in the field of watermarking so in order to achieve these two properties of watermark, Discrete wavelet transformation method and spread spectrum method are used in this paper. Discrete wavelet Transformation is used because wavelets process data at different scales or resolutions thus highlighting both small and large features [2]. The reason behind using spread spectrum sequences such as PN sequence is due to its good correlation properties [3]. This paper is organized as follows: Section II describes the Discrete wavelet transformation and section III describes the spread spectrum method. Section IV proposes the watermark embedding and extraction algorithm. Section V presents the results and discussions. Finally the conclusion is provided in section VI.

#### A. Wavelet

Wavelet is a finite energy function with zero mean and is normalized. A family of wavelets can be obtained by scaling and translating it. The continuous wavelet transform (CWT) of finite energy is the sum over all time of scaled and shifted versions of the mother wavelet  $\psi$  for a 1-D signal. In order for the wavelet transforms to be calculated using computers the data must be discretized. A continuous signal can be sampled so that a value is recorded after a discrete time interval. If the sampling of the signal is carried out at Nyquist rate, no information would be lost. After sampling the discrete wavelet series could be used. However, this can still be very slow to compute. The reason is that the information available through evaluation of wavelet series is still highly redundant and the solution requires a large amount of computation time. In order to make the wavelet computationally simple, a discrete algorithm is needed. The Discrete Wavelet Transform (DWT) provides sufficient information both for analysis and synthesis of the original signal with a significant reduction in the computation time. In

DISCRETE WAVELET TRANSFORMATION

addition, DWT is considerably easier to implement in comparison to the CWT.

The discrete wavelet analysis can be treated and implemented as band pass filters. Filters of different cutoff frequencies analyze the signal at different scales. Resolution is changed by filtering whereas the scale is changed by up and down sampling. If a signal is put through two filters: a high-pass filter (high frequency information is kept, low frequency information is lost) and a low pass filter (low frequency information is kept, high frequency information is lost), the signal is effectively decomposed into two parts, a detailed part (high frequency part), and an approximation part (low frequency part). The DWT of a 1-D (one dimension) signal x is calculated by passing it through a series of filters. First the samples x[k] are passed through a low-pass filter with impulse response 'g' resulting in a convolution of the two. The signal is also decomposed simultaneously using a high-pass filter with impulse response h. The output gives the detail coefficients (from the high-pass filter) and approximation coefficients (from the low-pass filter) as shown in Figure 1.



Figure 1: Block diagram of filter analysis (DWT)

It is important that the two filters are related to each other and they are known as a Quadrature Mirror Filter (QMF). However, since half the frequencies of the signal have now been removed, half the samples can be discarded according to Nyquist rule. The filter outputs are then down sampled by a factor of 2. This decomposition is repeated to further increase the frequency resolution and the approximation coefficients are decomposed with high and low pass filters and then down sampled. DWT is one of the well-known techniques for subband image coding. It decomposes the original image iteratively into a group of transform coefficients and these coefficients are called subbands. DWT subband decomposition of image separates image data into high and low frequency bands using high-pass and low-pass filtering followed by down sampling to remove redundant data. Decoding on the other hand involves upsampling to adjust dimensionality and recombining data from different bands. For a 2-D signal such as image, first level decomposition will result into four components as shown in Figure 2.



Figure 2: One-level subband decomposition

Application of DWT to an image involves combinations of the filters (combinations of the scaling function and the wavelet function) to produce unique subbands. The LL (low-low or approximation) subband is produced by low- pass filtering along the rows and columns, and it is commonly referred to as a coarse image approximation. The LH (low-high or vertical details) subband is produced by low pass filtering along the columns, thus capturing the horizontal edges. The HL (high-low or horizontal details) subband is produced by high-pass filtering along the rows and low pass filtering along the columns, thus capturing the vertical edges. The HH (high-high or diagonal details) subband is produced by high pass filtering along the rows and columns, thus capturing the vertical edges. The HH (high-high or diagonal details) subband is produced by high pass filtering along the rows and columns, thus capturing the diagonal edges. The LH and HL subbands are considered the band-pass subbands and the LH, HL, and HH subbands together are called the detail subbands [14]. The four subbands are shown in Figure 3.

| LL3 | HL3 | HL2 |     |  |
|-----|-----|-----|-----|--|
| LH3 | HH3 |     | HL1 |  |
| LH2 |     | HH2 |     |  |
| LH1 |     |     | HH1 |  |

#### Figure 3: Pyramid Structure of Three level DWT

The LL subband contains average coefficients that have greater part of original image energy and thus contains most of the information. By repeating the process on the LL subband, additional scales are produced.

## B. Haar Wavelet

The Haar wavelet uses a rectangular window to sample the time series such that the first pass over the time series uses a window width of two which is doubled at each step until the window encompasses the entire time series. Each pass over the time series generates a new time series and a set of coefficients. The new time series is the average of the previous time series over the sampling window. The coefficients represent the average change in the sample window. There are a wide variety of popular wavelet algorithms, including Daubechies wavelets, Mexican Hat wavelets and Morlet wavelets. These wavelet algorithms have the advantage of better resolution for smoothly changing time series. But they have the disadvantage of being more computationally complex than the Haar wavelets. In addition, the Haar wavelet transform is fast, memory efficient and exactly reversible without the edge effects that are present in other wavelet transforms.

It is evident that energy of an image is concentrated in the low frequency components. Thus lower sub band are more vulnerable to image alterations as compared to higher subbands. Therefore, watermark requires great robustness and is embedded at higher subbands. In general, horizontal and vertical subbands have more or less the same characteristics and behavior in contrast to diagonal ones. There upon, watermark embedding in the vertical and horizontal subbands guarantees increased robustness, since their energy compaction makes them less vulnerable to attacks. On the other hand, the coarse scale approximation includes most of the energy of the original image and has a crucial effect on image quality; therefore, it is not used for embedding in order to retain imperceptibility.

#### III. SPREAD SPECTRUM METHOD

Digital watermarking may not be secure despite its robustness. Therefore, security of the watermark becomes a critical issue in many applications. The problem of watermark security can be solved using spread-spectrum scheme. In this Method, the watermark is spread across the cover image by using more number of bits than the minimum required. This scheme of hiding the data uses the concept of code division multiple access (CDMA). This technique ensures the survival of watermark under various attacks due to redundancy. According to Shannon's approach, the watermarking technique is perfectly secured if and only if no information about the secret key leaks from the observations. The problem of watermark security can be solved using Spread Spectrum (SS) technique.

In SS watermarking technique, the transmitted or the narrowband signal is spread over a wide frequency band, which is much wider than the actual minimum bandwidth required, such that the signal energy presented in any signal frequency is undetectable [4]. This large bandwidth signal is called as the spreading signal. One way of widening the bandwidth is by the use of modulation. Pseudo Noise (PN) sequences are used as the spreading sequences.

A PN sequence is a sequence of binary numbers which appears to be random, but is in fact perfectly deterministic. The sequence appears to be random in the sense that the binary values and groups or runs of the same binary value occur in the sequence in the same proportion. For watermarking application, a pseudorandom number generator is used to determine the pixels for embedding the watermark data using a "key". Following are the properties of PN Sequences [12]:

• Balance Property: This property states that in the sequence generated the number of ones is equal to the number of zeros.

- Run Property: A run is a sequence of a single type of binary digits. Among the runs of ones and zeros in each period it is desirable that about one-half the runs of each type are of the length 1, about one-fourth are of length 2, one-eight are of length 3, and so on.
- Shift Property: This property states that for any sequence and its cyclically shifted sequence the agreements and disagreements among them will be approximately equal.
- Autocorrelation property: The autocorrelation property is periodic and binary valued.
- Cross-correlation Property: The cross-correlation property provides a measure of resemblance between two different sequences.

These properties make SS very popular in present-day digital watermarking. PN sequences are a good tool for watermarking because of the following reasons:

- PN sequence is having correlation properties, noise like characteristics and resistance to interference.
- PN generator produces periodic sequences that appear to be random.
- PN sequences are generated by an algorithm that uses an initial seed.
- The PN sequence generated is actually not statically random but will pass many test of randomness.
- Unless the algorithm and seed are known, the sequence is impractical to predict.

PN sequences can be generated by using a Linear Feedback Shift Register (LFSR) circuit i.e. when a shift register has a non-zero initial state and the output is fed back to the input, the unit acts as a periodic shift register. Figure 4 shows a LFSR that uses a three stage shift register where the second and the third cells are tapped and modulo-2 added and fed back to the first stage i.e.



Figure 4: Linear Feedback Shift Register

The contents of the shift register are shifted with each clock pulse. The output of the LFSR is taken from the M3 stage. The output of the three shift registers is shown in the Table 1 below. The output from the LFSR is a seven bit sequence  $1\ 1\ 1\ 0\ 0\ 1\ 0$ , which repeats periodically thereafter.

| M1 | M2 | M3 |
|----|----|----|
| 1  | 1  | 1  |
| 0  | 1  | 1  |
| 0  | 0  | 1  |
| 1  | 0  | 0  |
| 0  | 1  | 0  |
| 1  | 0  | 1  |
| 1  | 1  | 0  |
| 1  | 1  | 1  |

Different sequences can be created by extending the PN sequences which can provide more correlation and security in terms of watermarking. Following is the discussion of such sequences:

- Random Sequence: In random binary sequence, sequence is generated randomly i.e. system randomly sets the contents of the register. Only the length of sequence along with the state is provided.
- Maximal Length Sequence: For Maximal Length (M) Sequence, feedback shift register is used[18]. It consists of a shift register made up of m flip flops and a logic circuit. The flip flops in the shift register are regulated by a single timing clock. Binary registers are shifted through the shift registers and the output of the various stages are logically combined and feedback as the input to the first stage.

In M-sequence, initial contents of the flip flops are given which determine the contents of the memory, length of the shift register and feedback logic which consists of exclusive OR gates. The M sequence will be produced by XORing the contents of the flip flops every time fed by the feedback logic.

- Gold Sequence: The autocorrelation properties of m-sequence cannot be bettered but they don't exhibit good cross-correlation properties for CDMA. It's known that, a set of spreading codes used for multiple access system should have as little mutual interference as possible. For this reason, a particular class of PN sequences is used that are called Gold sequences. They can be chosen such that, the cross-correlation values between the codes over a set of codes are uniform and bounded. Gold codes can be generated by modulo-2 addition of two maximum-length sequences with the same length. The code sequences are added chip by chip by synchronous clocking. The generated codes are of the same length as the two m-sequences which are added together [4].
- Kasami Sequence: Kasami sequence sets are one of the important types of binary sequence sets. To generate a Kasami sequence, first of all a m sequence is created which is then XORed with other m-sequence a'. The second m-sequence a' is created by taking the sample period of 2^ (length (a)/2) +1 i.e. selecting every (2n/2+1)st bit of an m-sequence a. The resulting sequence a' is an m-sequence. The Kasami sequence can then be obtained by adding (modulo-2 addition) the sequences a and a'. Then by adding all cyclic shifts of the sequence a' with the sequence a, a new set of Kasami sequences can be formed [11].

### IV. PROPOSED WORK

The Proposed method decomposes cover image (original image), which is to be watermarked using DWT. The watermark is embedded to the specified DWT coefficient of the cover image. A new DWT based spread spectrum watermarking technique is proposed on the basis of embedding of various sequences in the DWT coefficients. The algorithm is Column wise DWT Coefficients Embedding Algorithm (CCE). In this method columns of DWT coefficients are taken for watermarking. The proposed algorithm is experimented on different sequences. Performance of the algorithm is analyzed by varying the gain factor and by inserting different sequences. Simulation results show that the proposed method achieves higher security and robustness especially in the case of Kasami sequence. This section improvises the proposed DWT based spread-spectrum watermarking technique by altering the coefficient's matrix column wise. Watermarking is having two phases. The first phase is called embedding and second phase is called recovery. Both these phases are described below along with the proposed algorithm.

a. Embedding

The input to the embedding process is the gray scale host image and the watermark image that is to be embedded into the host image. The output of the embedding process is the watermarked image i.e. the image that contains the watermark. The proposed scheme invisibly embeds the gray scale watermark into the host image which makes the information about the authentication more secure. Before embedding procedure, binarization of watermark (message vector) is done. The subband decomposition is performed on the cover image using Haar wavelet transform which would result into four subbands namely LL, HL, LH and HH.

Among these subbands, HL (Horizontal subband) and LH (vertical Subband) are taken and combined and a concatenated subband will get generated. A Pseudo Noise (PN) sequence, which can be a random sequence, m-sequence, gold sequence and Kasami sequence, of size identical to the concatenated subband column size is produced and a secret key is used, which is required to be known at detector for the extraction process. Based on the value of the bit for the message vector, the PN sequence is then added/subtracted to/from the concatenated subband columns according to the data embedding rule as follows:

$$W=V+k*X \text{ if } b=1$$
 (2)

Where V is the concatenated subband wavelet coefficient of the cover image, W is the wavelet coefficient after watermark embedding, k is the gain factor, X is the PN sequence and b is the bit of watermark that has to be embedded. Generation of PN sequences for embedding each bit enhances the security of the

(3)

watermarking algorithm. The final modified coefficients are then reconverted back to LH and HL subbands and the watermarked image is created by using inverse DWT transform.

## b. Recovery

Various attacks are applied to the watermarked image and the image that is obtained after applying an attack on the watermarked image is called attacked image. The input to the watermark extraction process is the attacked image and the size of the watermark. Since the watermark extraction process does not require the original image, so the proposed scheme comes under the category of blind watermarking. The output of the extraction process is the original watermark.

To detect the watermark, the watermarked image is decomposed into four subbands and out of these subbands LH and HL are concatenated. The watermark signal is usually applied to middle frequencies of the image, keeping visually the most important parts of the image (low frequencies) and avoiding the parts presented by high frequencies which are easily destructible by compression or scaling operations. The same pseudo noise sequence (random sequence, m-sequence, gold sequence, and Kasami sequence) which is used during insertion of watermark is generated by using same state key and then its correlation with the corresponding column of the concatenated subbands DWT coefficients is determined. Mean of the correlation values is taken as threshold T for message extraction. During detection, if the correlation value of a particular column exceeds T for a particular sequence then "1" is recovered, otherwise "0" is recovered. The recovery process is then iterated through the entire PN sequence until all the bits of the watermark has been recovered.

c. Watermark Embedding Algorithm

Step I: Read the gray scale image as host image of size M\*N and a gray scale image as the watermark.

Step II: Reshape the watermark into message vector of 1's and 0's.

- Step III: Perform DWT on the host image to decompose it into four non overlapping multiresolution coefficient sets LL, LH HL and HH.
- Step IV: Concatenate the subbands LH and HL. The size of the plane will be M/2 \* N.
- Step V: Generate a pseudo noise sequence of size identical to the concatenated subband column size.
- Step VI: Perform the following operations based on the watermark bit:
  - (i) For watermark bit '1' add the Pseudo noise sequence to the concatenated subband column.
  - (ii) For watermark bit '0' subtract the Pseudo noise sequence from the concatenated subband column.

$$W=V+k*X for b=1 W=V-k*X for b=0$$

Where W is the wavelet coefficient after embedding, V is the concatenated subband wavelet coefficient of the cover image, k is the gain factor, X is the PN sequence and b is the bit of watermark that has to be embedded.

Step VII: Key and Gain factor are fixed before the generation of PN sequence

Step VIII: Divide the concatenated Subbands into LH and HL again of respective size.

Step IX: Perform the inverse wavelet transformation to get the watermarked image.

- d. Watermark Extraction Algorithm
- Step I: Read the watermarked image and size of the watermark.
- Step II: Perform DWT on the watermarked image to decompose it into four non overlapping multiresolution coefficient sets LL, LH HL and HH.
- Step III: Concatenate the subbands LH and HL. The size of the plane would be M/2 \* N.
- Step IV: Generate same pseudo noise sequence which was generated during embedding process using same key.
- Step V: Determine the PN sequence correlation with the corresponding column of the concatenated subbands DWT coefficients.
- Step VI: Mean of the correlation values is taken as threshold T for message extraction.
- Step VII: Perform the following to extract watermark
  - (i) If the correlation value for a particular column exceeds T then '1' is recovered.
  - (ii) If the correlation value for a particular column does not exceed T then '0' is recovered.
- Step VIII: The recovery process is then iterated through the entire PN sequence until all the bits of the watermark has been recovered.
- Step IX: Reshape the extracted sequence and display the recovered watermark.

#### V. RESULTS AND DISCUSSION

The proposed watermarking scheme is invisible, blind and robust. To verify the effectiveness of the proposed method, a series of experiments are conducted on several test images. In the experiments, the test images or host images are gray scale images of standard size whereas the watermark image is a gray scale image which is converted into a message vector. The watermark is embedded effectively into the host image and on the other hand, the embedded watermarks are extracted efficiently from the watermarked images. For each test image, the results of proposed watermark embedding and extraction algorithms are compared for different sequences. Since the proposed watermarking scheme is invisible, so the watermarked images seem to be exactly similar to the original host image.

The values of quality metrics for the host image CT are shown in Table 2. In this table result is calculated by varying the gain factor 'k' which can be viewed as a relative measure of embedding strength. A small value of k will cause perceptual degradation in the watermarked image. Perceptual quality of watermarked image is measured by calculating Peak Signal to Noise Ratio(PSNR) between cover and watermarked image which should be high. At receiver side, watermark is extracted from the watermarked image. Evaluation of extracted watermark is done by measuring correlation with the original watermark which should be 1 or near to 1. The formula for PSNR and Correlation is given below:

$$PSNR = \frac{10 * \log_{10} (max ((x (i, j))^{2}))}{MSE}$$
(4)  
$$MSE = \sum \sum ((x (i, j) - y (i, j))^{2} (5)$$
  
$$NM$$

Where x (i,j) is original image, y(i,j) is watermarked image and M\*N is the size of the image.

$$NC = \frac{\sum x (i, j)^* y (i, j)}{\sqrt{\sum \sum x (i, j) 2 * \sum x (i, j) 2}}$$
(6)

Where x(i,j) is original watermark, y(i,j) is recovered watermark, M\*N is size of the image.

From the table, it can be verified that PSNR and Correlation values for the proposed algorithm are better in case of Kasami sequence as compared to other sequences. For correlation to be better it should have value '1'.Table 3 show the results obtained after applying attacks for the host image CT. To do the comparison, a number of attacks have been applied on the watermarked image. The attacks used are Gaussian noise, salt and pepper noise, speckle noise, contrast enhancement, histogram equalization, edge sharpening, Gaussian low pass filter, wiener filter and laplacian high pass filter. Then the quality of the watermark extracted from the attacked image using the proposed method has been checked by finding the values of Correlation between original watermark and extracted watermark. As it is clear from this table that correlation is mostly 1 or close to 1 which means that the proposed method is more robust against attacks. Table 4 and 5 shows the visual results of watermarked image and retrieved watermark for CT image respectively after applying all the attacks.

| Gain Factor | Sequences       | PSNR    | Correlation |  |
|-------------|-----------------|---------|-------------|--|
|             | M-sequence      | 48.1308 | 0.9722      |  |
| K=1         | PN sequence     | 49.5298 | 0.9764      |  |
|             | Gold Sequence   | 51.1411 | 0.9799      |  |
|             | Kasami Sequence | 53.8881 | 0.9870      |  |
|             | M-sequence      | 34.1514 | 1           |  |
|             | PN sequence     | 35.5504 | 1           |  |
| K=5         | Gold Sequence   | 37.1617 | 1           |  |
|             | Kasami Sequence | 39.9087 | 1           |  |
|             | M-sequence      | 28.1308 | 1           |  |
| K=10        | PN sequence     | 29.5298 | 1           |  |
|             | Gold Sequence   | 31.1411 | 1           |  |
|             | Kasami Sequence | 33.8881 | 1           |  |

Table 2: Comparison of results for CT image by varying the gain factor 'k'

Table 3: Comparison of Experimental results from attacked CT image at gain factor k=5

|                               | Correlation |             |               |                    |  |
|-------------------------------|-------------|-------------|---------------|--------------------|--|
| Attack                        | M-sequence  | PN sequence | Gold sequence | Kasami<br>Sequence |  |
| Gaussian Noise                | 0.9652      | 0.9672      | 0.9771        | 0.9779             |  |
| Salt and Pepper Noise         | 0.9803      | 0.9816      | 0.9853        | 0.9875             |  |
| Speckle Noise                 | 0.9929      | 0.9952      | 0.9953        | 1                  |  |
| Contrast<br>Enhancement       | 0.9977      | 1           | 1             | 1                  |  |
| Histogram<br>Equalization     | 1           | 1           | 1             | 1                  |  |
| Edge Sharpening               | 0.9840      | 0.9861      | 0.9780        | 0.9892             |  |
| Gaussian Low pass<br>Filter   | 0.9952      | 0.9976      | 1             | 1                  |  |
| Wiener Filter                 | 0.9073      | 0.9300      | 0.9393        | 0.9489             |  |
| Laplacian High Pass<br>Filter | 1           | 1           | 1             | 1                  |  |

|                             | Watermarked Image |  |               |                 |  |  |
|-----------------------------|-------------------|--|---------------|-----------------|--|--|
| Attacks                     | M-sequence        | PN sequence  | Gold Sequence | Kasami Sequence |  |  |
| No Attack                   |                   | Destinged<br>Provide and the second sec |               |                 |  |  |
| Gaussian<br>Noise           |                   |  |               |                 |  |  |
| Salt and<br>Pepper<br>Noise |                   |  |               |                 |  |  |
| Speckle<br>Noise            |                   |  |               |                 |  |  |

Table 4: Comparison of visual quality of watermarked image

| Contrast<br>Enhanceme<br>nt    |  |  |  |
|--------------------------------|--|--|--|
| Histogram<br>Equalization      |  |  |  |
| Edge<br>Sharpening             |  |  |  |
| Gaussian<br>Low Pass<br>Filter | SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOLSE<br>SCHOOL | EXERCISIVE<br>FOR THE INTERNAL IN MERINAL THE PROPERTIES AND |  |
| Wiener<br>Filter               |  |  |  |



Table 4.12: Comparison of visual quality of watermarks extracted from attacked CT image

|                              | Extracted Watermark |                        |               |                    |
|------------------------------|---------------------|------------------------|---------------|--------------------|
| Attacks                      | M-sequence          | PN sequence            | Gold Sequence | Kasami<br>Sequence |
| No Attack                    | SHIVANY             | SHIY ANG               | SHIY ANG      | SHIYANS            |
| Gaussian Noise               | 34144144            | 5HI¥ AN4               | SHIY ANY "    | SHIY ANY           |
| Salt and Penner Noise        | SHIVANI             | SHIY ANS               | SHIY ANG      | SHIYANY            |
| Speckle Noise                | SHIVANY             | SHIY ANG               | SHIY ANG      | SHIY ANG           |
| Contrast Enhancement         | SHIVANY             | SHIY ANG               | SHIY ANG      | SHIY ANG           |
| Histogram Equalization       | SHIYANY             | SHUYÀNY                | 5H14 AN4      | 5HI4 AM4           |
|                              | SUILANI,            | SKANN .                | SHILLANS .    | <b>SHYDNN</b>      |
| Gaussian Low Pass            | SHIYANI             | SHI VANG               | SHIY ANI      | SHIVANA            |
| Wiener Filter                |                     |                        | SH Park       | Sliffers .         |
| Laplacian Low Pass<br>Filter | ·5HIYAN4            | . <sup>5</sup> 814,4N4 | SHIYANI       | ·SHIYANI           |

It is clear from the results that watermark survives against a large number of attacks in case of all sequences of proposed scheme. But among all the sequences Kasami sequence has given better results than other sequences. So it has been verified that the proposed scheme is more robust for Kasami sequence than other sequences.

#### VI. CONCLUSION

In the proposed work an efficient watermarking scheme and efficient sequence in transform domain for authentication of digital images is represented. Since the watermark embedded by the proposed scheme is invisible to human eyes, so the watermarking scheme proposed in this work comes under the category of invisible watermarking. As the proposed watermarking scheme is blind, the extraction of watermark requires only the watermarked image and it neither demands the original image nor original watermark. Experimental results show that watermarked image and watermark obtained using the proposed scheme is in good visual quality.

The main objective of this work is to provide robustness and security. As among transform domains, Discrete Wavelet Transform has proved high robustness so the proposed work also makes the use of wavelets and getting the better results. Moreover security is increased by the use of spread spectrum technique which makes use of a sequence. Four different sequences are used, and it is concluded that Kasami sequence gives better results than other sequences.

#### REFERENCES

- [1] Chavan, S.K., Shah, R., Poojary, R., Jose, J. and George, G., 2010. "A Novel Robust Colour Watermarking Scheme for Colour watermark images in Frequency Domain", Proceedings of IEEE International Conference on Advances in Recent Technologies in Communication and Computing.
- Chouhan, R., Mishra, A. and Khanna, P., 2011. "Wavelet-based robust digital watermarking scheme for fingerprint authentication", [2] Proceedings of International Conference on Intelligent Computational Systems (ICICS), pp. 29-33. Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T.G., 1997. "Secure Spread Spectrum Watermarking for multimedia", Proceedings of
- [3] IEEE International Conference on Image Processing, Vol. 6, pp. 1673-1687.
- Fang, Y., Huang, J. and Shi, Y.Q., 2003. "Image Watermarking Algorithm Applying CDMA", IEEE International Symposium on [4] Circuits and Systems, Vol.2.
- [5] Hameed, K., Mumtaz, A. and Gilani, S.A.M., 2006. "Digital Image Watermarking in the Wavelet Transform Domain", Proceedings of IEEE World Academy of Science, Engineering and Technology.
- [6] Joseph, J. K. and Dowling, W.J., 1998. "Rotation, scale and translation invariant spread spectrum digital image watermarking", Signal Processing, 66(3): 303-3 17.
- Katzenbeisser, S. and Peticolas, F.A.P., 2000. "Information Hiding Techniques for Steganography and Digital Watermarking", [7] Artech House Publishers.
- Kesidis, L. and Gatos, B., 2007. "A Robust Image Watermarking Technique Based on Spectrum Analysis and Pseudorandom [8] Sequences", VISAPP, 2nd International Conference on Computer Vision Theory and Applications, Barcelona, Spain.
- Khalili, M., 2011. "A secure and robust cdma digital image watermarking algorithm based on dwt2, YIQ color space and Arnold [9] transform", Signal & Image Processing: An International Journal (SIPIJ) Vol.2, No.2.
- [10] Kumar, B., Anand, A., Singh, S.P. and Mohan, A., 2011. "High Capacity Spread-Spectrum Watermarking for Telemedicine Applications", Proceedings of IEEE World Academy of Science, Engineering and Technology.
- [11] Mitr, A., 2008. "On Pseudo-Random and Orthogonal Binary Spreading Sequences", International Journal of Information and Communication Engineering.
- [12] Penumarthi, K. and Kak, S., 2006. "Augmented Watermarking", Cryptologia, 30:173–180.
  [13] Rosa L., 2009. "High Capacity Wavelet Watermarking Using CDMA Multilevel Codes", Citeseerx.
- [14] Sharkas, M., ElShafie, D. and Hamdy, N., 2005. "A Dual Digital-Image Watermarking Technique", Proceedings of IEEE World Academy of Science, Engineering and Technology.
- [15] Su, G., 2008. "An Overview of Transparent and Robust Digital Image Watermarking", Citeseerx.
   [16] Thanki, R.M., Kher, R.K. and Vyas, D.D., 2011. "Robustness of Correlation Based Watermarking Techniques Using WGN against Different Order Statistics Filters", International Journal of Computer Science and Telecommunications, Volume 2, Issue 4. [17] Todorov, T., 2004. "Spread spectrum watermarking technique for information system securing", International Conference on
- Computer Systems and Technologies CompSysTech.
- Van Schyndel, R.G., Tirkel, A.Z. and Osborne, C.F., 1994. "A digital watermark", Proceedings of IEEE International Conference on Image Processing, Vol. 2, pp. 86-90. [18]
- [19] Verma, H.K., Singh, A.N. and Kumar, R., 2009. "Robustness of the digital Image Watermarking Techniques against Brightness and Rotation Attack", International Journal of Computer Science and Information Security, Vol. 5, No. 1.
- [20] Xia, X., Boncelet, C.G. and Arce, G.R., 1997. "A Multiresolution Watermark for Digital Images", Proceedings of IEEE International Conference on Image Processing. Xiwen, S., 2010. "The application of digital watermarking technology in the field of e-commerce", Proceedings of IEEE International
- [21] Conference on Information Management, Innovation Management and Industrial Engineering.