International Journal of Electrical, Electronics and Computer Engineering **7**(2): 42-50(2018)

ISSN No. (Online): 2277-2626

Digital Water Marking Techniques and Uses intellectual property rights

***Nandan Kumar*[1] *and Prof. Sneha Jain*[2]**

[1]Research Scholar, Department of Electronics and Communication Engineering,
RITS, Bhopal, (Madhya Pradesh), India
[2]Assistant Professor, Department of Electronics and Communication Engineering,
RITS, Bhopal, (Madhya Pradesh), India

(Corresponding author: Nandan Kumar)

(Received 07 August, 2017 Accepted 20 October, 2018)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Digital Water Marking Techniques and Uses intellectual property rights development in software technologies has necessitated the owner to pay great attention in protecting their intellectual property rights (IPR). Watermarking is used to protect IPRs for content authentication and ownership protection. Demand for software protections such as copyright and anti-tampering defense are becoming more important to software users and developers. Software watermarking is a software-based technique to protect software from piracy. In this work, study of watermarking, software watermarking and security issues for business software, browser based online applications and relational databases has been done.

Watermarking is not a new technique while it was used from long year ago for the purpose of copyright protection and authentication. This technique also makes an attempt to determine the problems associated with the management of property of media. In this paper, block cipher and spread spectrum technique is proposed for watermarking. The proposed approach is a combinatorial strategy for applying compression, encryption and watermarking for the fruitful counteractive action from different attacks in the system. The simulation of proposed approach is done in MATLAB simulator and the imperceptibility and sturdiness of the watermarked image is checked out by measuring the PSNR, MAE, NAE and NCC. The simulation result of proposed approach gives improved results than the existing system and it is much more effective to reduce the noise and error on the image.

Keywords: Block Cipher, Copyright protection, Digital Image Watermarking. MATLAB, Spread Spectrum

I. INTRODUCTION

Owing to the popularity of the Internet and the rapid growth of multimedia technology, users have more and more chances to use multimedia data. Consequently, the protection of the intellectual property rights of digital media has become an urgent issue. Digital watermarking has attracted considerable attention and has numerous applications, including copyright protection, authentication, secret communication, and measurement [1-2]. According to the domain in which the watermark is inserted, these techniques are classified into two categories, i.e., spatial-domain and transform-domain methods. Embedding the watermark into the spatial-domain component of the original image is a straightforward method. It has the advantages of low complexity and easy implementation. However, the spatial-domain methods are generally fragile to image-processing operations or other attacks.

Watermarking infers the presence of a mark in multimedia substance, which contains the author's name, his signature or mark. Client of substance can't see the embedded watermark [3].

The algorithm for embedding an imperceptible watermark depends on the engravings of the watermark in the frequency domain. In the frequency domain watermarking is harder to separate without abusing the nature of the watched picture. The application of the three fundamental sorts of transformation: Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are displayed in the literature [4-6]. It has been demonstrated that DWT acquires the most prevalent outcomes in including an undetectable watermark. Despite the strategy for information appropriation and the quantity of duplicates made, the chief objective of the watermark engraving is to accomplish validation.

The author has introduced diverse methods to watermark the images. This paper is centered on watermark embedding based on block cipher and spread spectrum technique. Contingent upon the connected spread spectrum methods certain algorithm will have comparable qualities as when considering a radio framework that applies the important procedures of spread spectrum.

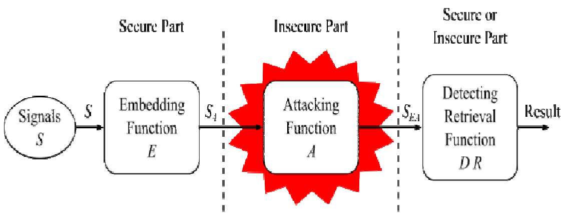


Fig. 1. Digital Image Watermarking Process.

The paper is organized as follows. In Section I the introduction about watermarking and spread spectrum is discussed. Digital watermarking techniques is discussing in Section II. The proposed methodology and its related algorithm are presented in Section III. In section IV experimental and its analysis is between performance metrics is discussing and Concluding remarks are presented in Section V.

II. WATERMARKING TECHNIQUES

There are many algorithms which are being used to hide the secret information. These algorithms can be categorized into two domains called:
1. Spatial domain and
2. Frequency domain.

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. On the other side, in frequency domain techniques the image is first transformed to the frequency domain by the use of any transformation methods such as Fourier transform, discrete cosine transform (DCT) or discrete wavelet transform (DWT). Now the information is added to the values of its transform coefficients. After applying the inverse transform, the marked coefficients form the embedded image.

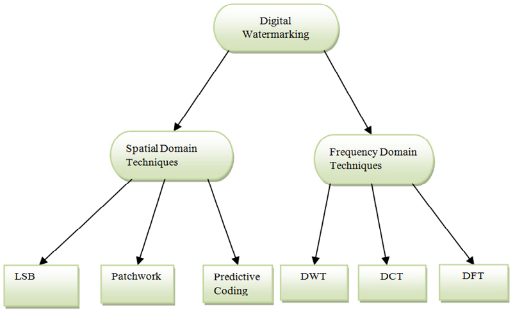


Fig. 2. Classification of Digital Watermarking.

A. Spatial Domain [7]

Least Significant bit (LSB). In this technique watermark is embedded in the LSB of pixels. Two types of LSB techniques are proposed. In the first method the LSB of the image was replaced with a pseudo-noise (PN) sequence while in the second a PN sequence was added to the LSB. This method is easy to use but not very robust against attacks.

Patchwork Technique. In patchwork, *n* pairs of image points, (a, b), were randomly chosen. The image data in *a* were lightened while that in *b* were darkened .High level of robustness against many types of attacks are provided in this technique. But here in this technique, very small amount of information can be hidden.

Predictive Coding Scheme. In this method, a pseudorandom noise (PN) pattern says W(x, y) is added to cover image. It increases the robustness of watermark by increasing the gain factor. But due to high increment in gain factor, image quality may decrease.

B. Frequency Domain

Discrete Cosine Transform [8]. The high frequency components are watermarked in frequency domain. The main steps are

1) Divide the image into non-overlapping blocks of 8x8
2) Apply forward DCT to each of these blocks
3) Apply some block selection criteria (e.g. HVS)
4) Apply coefficient selection criteria (e.g. highest)
5) Embed watermark by modifying the selected coefficients.
6) Apply inverse DCT transform on each block

DFT Domain Watermarking. DFT domain is favorite choice of researches because it provides robustness against geometric attacks like translation, rotation, cropping, scaling etc. There are two types of DFT based watermark embedding techniques. In first technique watermark is directly embedded and another technique is template based embedding. In direct embedding watermark is embedded by changing the phase information within the DFT [12].

A template is a structure which is used in the DFT domain to judge the transformation factor. First a transformation is made in image then to resynchronize the image this template is searched, and then employ the detector to extract the embedded spread spectrum watermark.

Discrete Wavelet Transform. Discrete wavelet transform is applied to decompose any non-stationary signal like an image, audio or video signal. The transform is predicated on little waves, known as wavelets, of varying frequency and limited duration. Frequency as well as spatial information of an image is retained during wavelet transformation. Temporal information is preserved during this conversion method [9]. Wavelets are made by translations and dilations of constant function called mother wavelet. DWT is performed by low-pass and high-pass filtering of an image. High-pass filter creates detailed image pixels and low-pass filter creates coarse approximation image pixels [10]. The outputs are down-sampled by 2 after performing the low-pass and high-pass filtering. 2D DWT is done by executing 1DDWT on each row, which is known as horizontal filtering and then on each column, which is known as vertical filtering [11].

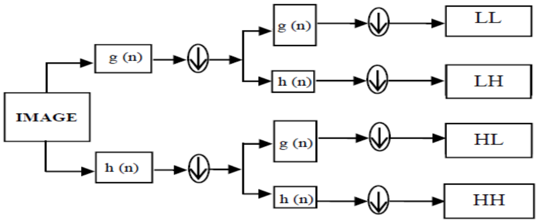


Fig. 3. 2D-DWT decomposition of an input image using filtering approach.

III. PROPOSED METHODOLOGY

This chapter discussed about the methodology for archiving target results along with proposed methodology.

A. Proposed Method

The proposed methodology implemented here for the information hiding using a hybrid combinatorial method of applying compression to the image and then encryption is done on the compressed image so that the information hide is made secure from various attacks. Finally the encrypted image is watermarked with the cover image using Spread Spectrum based watermarking.

The proposed methodology implemented here works in the following stages:

1. Input a cover image.
2. Apply JPEG-2000 compression and proposed JPEG-2000 compression generates a series of more than 90 different level of compressed image.
3. input secret image.
4. Apply Block cipher encryption on highly compressed image and also in secret image.
5. Finally encrypted image stored separately on disk.
6. Then the encrypted is watermarked with the cover image to get the resultant watermarked image.
7. Now for the retrieval of information from the watermarked image needs to apply reverse procedure.
8. The received watermarked image is then decrypted using the same Block Cipher technique, and generates cover image as well as secret image.
9. Decrypted image decompression is done by JPEG-2000 technique.
10. Then information retrieval is done using spread spectrum watermarking.

Input Image & Secrete Image. For the testing of the proposed methodology several Gray scale and Color images are taken from various sources of various types. The images include high dynamic images as well as Gray level images and Color images so that the proper working of the methodology is computed.

JPEG-2000 Compression Technique. The figure shown below is the standard architecture or the working of the proposed JPEG-2000 compression technique. The compression technique proposed consists of various phases such as preprocessing, DWT and quantization and arithmetic coding and bit-stream organization. The input JPEG 2000 image may contains one or more number of components. Since a typical color image contains three components i.e. RGB or YCbRr.

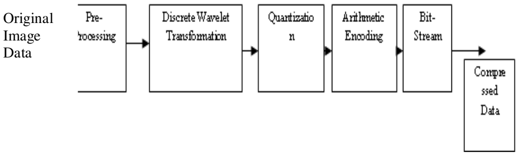


Fig. 4. Flow chart of the JPEG-2000 Compression Technique.

Pre-Processing. The pre-processing is the first stage of the jpeg-2000 compression which includes the partition of input image into number of rectangular and non-overlapping tiles of equal size. The size of the tiles depends on the size of the original input image. Each tile is compressed independently using its own set of specified compression parameters. Tiling is particularly useful for applications where the amount of available memory is limited compared to the image size.

Now the unsigned samples from each of the components are level shifted by subtracting a fixed value of 2^{B-1} from each of the sample to make its value symmetric around zero. Signed sample values are not level shifted. Similar to the level shifting performed in the JPEG standard, this operation simplifies certain implementation issues (e.g., numerical overflow, arithmetic coding context specification, etc.), but has no effect on the coding efficiency. Part 2 of the JPEG 2000 standard allows for a generalized DC offset, where a user defined offset value can be signaled in a marker segment.

Finally, the level-shifted values can be subjected to a forward point-wise inter component transformation to decorrelate the color data. One restriction on applying the inter component transformation is that the components must have identical bit-depths and dimensions. Two transform choices are allowed in Part 1, where both transforms operate on the first three components of an image tile with the implicit assumption that these components correspond to red–green–blue (RGB). One transform is the irreversible color transform (ICT), which is identical to the traditional RGB to YCbCr color transformation and can only be used for lossy coding. The forward ICT is defined as:

$$\begin{pmatrix} Y \\ C_b \\ C_r \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.16875 & -0.33126 & 0.500 \\ 0.500 & -0.41869 & -0.08131 \end{pmatrix} * \begin{pmatrix} R \\ G \\ B \end{pmatrix}$$

The above defined equation can be written as:

$$Y = 0.299(R - G) + G + 0.114(B - G),$$

$$C_b = 0.564(B - Y), C_r = 0.713(R - Y),$$

While the inverse ICT is given by

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} = \begin{pmatrix} 1.0 & 0 & 1.402 \\ 1.0 & -0.34413 & 0.71414 \\ 1.0 & 1.772 & 0 \end{pmatrix} * \begin{pmatrix} Y \\ C_b \\ C_r \end{pmatrix}$$

The other transform is the reversible color transform (RCT), which is a reversible integer-to integer transform that approximates the ICT for color de-correlation and can be used for both lossless and lossy coding. The forward RCT is defined as

$$Y = \left\lfloor \frac{R + 2G + B}{4} \right\rfloor, U = R = G$$
$$V = B - G$$

The Y component has the same bit-depth as the RGB components while the U and V components have one extra bit of precision. The inverse RCT, which is capable of exactly recovering the original RGB data, is given by

$$G = Y - \left\lfloor \frac{U + V}{4} \right\rfloor, R = U + G, B = V + G$$

At the decoder, the decompressed image is subjected to the corresponding inverse color transform if necessary, followed by the removal of the DC level shift. Since each component of each tile is treated independently, the basic compression engine for JPEG2000 will only be discussed with reference to a single tile of a monochrome image.

Discrete Wavelet Transformation. The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. In other words, this transform decomposes the signal into mutually orthogonal set of wavelets, which is the main difference from the continuous wavelet transform (CWT), or its implementation for the discrete time series sometimes called discrete-time continuous wavelet transform (DT-CWT).

The wavelet can be constructed from a scaling function which describes its scaling properties. The restriction that the scaling functions must be orthogonal to its discrete translations implies some mathematical conditions on them which are mentioned everywhere e. g. the dilation equation

$$\boldsymbol{\emptyset(x) = \sum_{k=-\infty}^{\infty} a_k \emptyset(S_x - k)}$$

Where S is a scaling factor (usually chosen as 2). Moreover, the area between the function must be normalized and scaling function must be orthogonal to its integer translates e. g.

$$\boldsymbol{\int_{-\infty}^{\infty} \emptyset(x)\emptyset(x + l)dx = \partial_{0,l}}$$

After introducing some more conditions (as the restrictions above does not produce unique solution) we can obtain results of all this equations, e. g. finite set of coefficients a_k which define the scaling function and also the wavelet. The wavelet is obtained from the scaling function as

$$\boldsymbol{\varphi(x) = \sum_{k=-\infty}^{\infty} (-1)^k a_{N-1-k}\, \varphi(2x - k)}$$

Quantization. The JPEG baseline system employs a uniform quantizer and an inverse quantization process that reconstructs the quantized coefficient to the midpoint of the quantization interval. A different step size is allowed for each DCT coefficient to take advantage of the sensitivity of the human visual system (HVS), and these step-sizes are conveyed to the decoder via an 8 * 8 quantization table (q-table) using one byte per element. The quantization strategy employed in JPEG2000 Part 1 is similar in principle to that of JPEG, but it has a few important differences to satisfy some of the JPEG2000 requirements.

Arithmetic Encoding. In Arithmetic Encoding , the idea of replacing an I/P symbols with a specific code is completely bypassed. Instead, a stream of I/P symbols replaced with a single floating point number in [0,1]. The O/P of an arithmetic coding is, as usual ,a stream of bits.

Bit Stream. A bit stream is a continuous sequence of bits, representing a stream of data, transmitted continuously over a communication path, serially one at a time. The longer and more complex the message, the more bits are needed to represents the O/P number.

Block Cipher Encryption. A block cipher operating on b-bit inputs is a family of permutations on b bits with the key given to the block cipher used to select the permutation.

k: q-bit key.

P: b-bit string denoting a plaintext.

C: b-bit string denoting a cipher text.

An encryption function: E = {E_k} is a family of 2^q permutations on b bits indexed by k, where k is q bits

A decryption function: D = {D_k} is a family of 2^q permutations on b bits indexed by k such that D_k is the inverse of E_k.

Given a b-bit plaintext, P, and key, k, if C = E_k(P) then P = D_k(C).

Spread Spectrum Watermarking

1. Take an input image and a secrete image.
2. Choose alpha value which denoted watermark signal strength factor in spread spectrum algorithm, here in our work we assume alpha=5;
3. Calculate DWT of the original image which is used for the transformation of the image to be embedded.
4. Calculate total number of pixels of the original image and watermark image.
5. Calculate aj=bj where ir<=j<(i+1)r.
6. Calculate watermark signal as wj=alpha*aj*pj, where pj= {+1,-1}.
7. Now we will find the kernel of the image by taking kernel size 31 and by taking the level of the kernel size as 3 we will find the kernel image of the original image by calculating kernel image = (1/(2*pi*s^2))*exp(-((X-m).^2 + (Y-m).^2)/(2*s^2));

8. This watermark signal is then embedded with the kernel image to get the final watermark image.

The embedding process is carried out by first generating the watermark signal W by using watermark information bits, chip rate and PN sequence. The watermark information bits b= {bi}, where bi = {1,-1} are spread by r, which gives

$$a_j = b_i, \qquad ir \leq j < (i+1)r$$

The sequence aj is then multiplied by alpha>0 and P. The watermark signal W= {wj},where

$$w_j = \alpha a_j P_j$$

Where, pj= {1,-1} the watermark signal generated is added to the encrypted signal, to give the watermarked signal Cw.

$$C_w = C + W = c_{wi} = c_i + w_i, \qquad \forall_i = 0,1, \ldots \ldots .., L-1$$

The encrypted value of M2 denoted by C2 is

$$c_{2i} = (m_{2i} + k_{2i}) mod\ 255 \ \ \forall_i = 0,1, \ldots \ldots ., L-1$$

Kernel Based Image Detection. In image processing, a kernel is simply a 2-dimensional matrix of numbers, therefore kernels are also known as convolution matrices or masks. Techniques such as blurring, edge detection and sharpening all depends on kernels .Kernels are applied across an image in order to process the image as a whole.

Following steps are followed for image detection:

1. ksize_image = 31;

It is the kernel size that we want to make the size of the kernel.

2. kernel = zeros(ksize_image);

Whatever the size of the kernel make the pixel value of all zeros.

3. s = 3;

It is the segmented part from the kernel image.

4. [X, Y] = meshgrid(1:ksize_image);

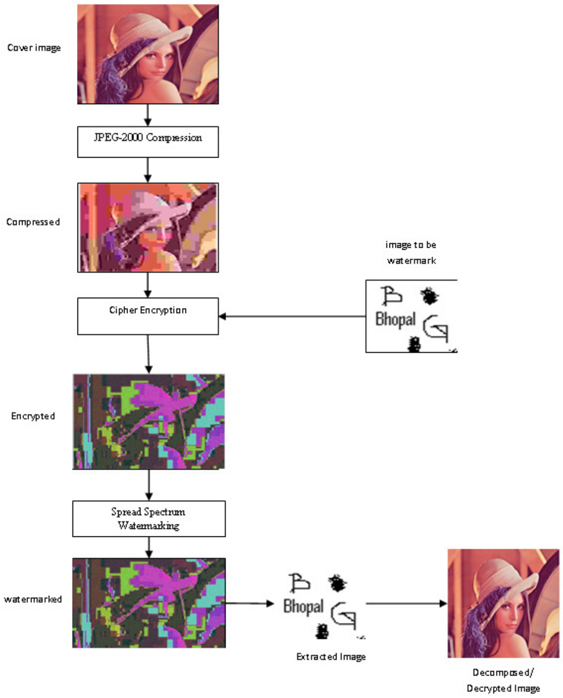
Generate X and Y arrays for 3-D plots from 1 to the size of the kernel and stores rows and columns in X and Y.

5. kernel_image = (1/(2*pi*s^2))*exp(-((X-m).^2 + (Y-m).^2)/(2*s^2));

Now calculate the original kernel by reducing the total size and the size of the kernel taken. Kernel image is used for the embedding of kernel region in the image the total effect of blurriness is pointed out so that it will be helpful for the detection of embedding part of the image.

Flow Chart of the Methodology. The proposed methodology applied here for the security of information that is hidden inside the original image is implemented here. The proposed methodology is a combinatorial method of applying compression, encryption and watermarking for the successful prevention from various attacks in the. The information to be hidden is first compressed using JPEG-2000 compression technique; JPEG-2000 compression generates a series of compressed images on the basis of compression ratio.

The most compressed image is then taken for further process. The compressed image is taken and is encrypted using block cipher. The encrypted image and the cover image is taken and watermarked, these two images to generate watermarked image using spread spectrum based watermarking. The flow chart shown below is the separate working process of the methodology.



IV. EXPERIMENTAL RESULTS

The experimental analysis of the proposed methodology is done using a widely used MATLAB2012A toolbox [13] and the machine configuration is Intel I3 core 2.20Ghz processor, with 4GB RAM, windows 7 home basis. In proposed methodology we applied a compression and encryption and watermarking for the successful prevention from various attacks in the network. The information to be hidden is first compressed using JPEG-2000 LS compression technique; JPEG-2000 LS compression generates a series of compressed images on the basis of compression ratio.

A. Snapshots

The figures shown below is the original image which needs to be watermarked. The figure 5 (a) shows the original cover image, figure 5(b) shows the compressed image and the figure 5 (c) show the compressed image including encrypted image.

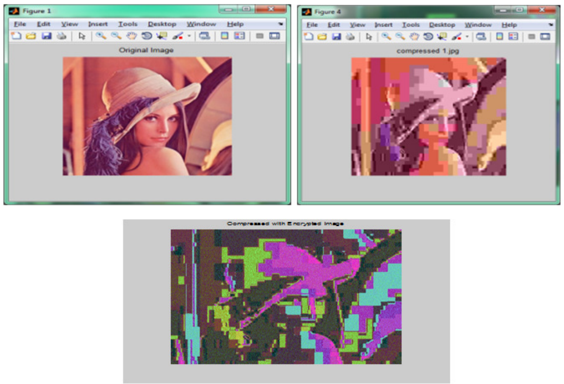


Figure 1
File Edit View Insert Tools Desktop Window Help
Original Image
Figure 4
File Edit View Insert Tools Desktop Window Help
compressed 1.jpg
Compressed with Encrypted Image

Fig. 5. a) original Image b) compressed image c) encrypted image.

The figure shown below is the image to be watermrked and the resultant watermarked image and the watermarked image containing noise. The figure 6(a) is the image to be watermarked figure 6 (b) shows the resultant watermarked image and figure 6 (c) is the watermarked image with noise.

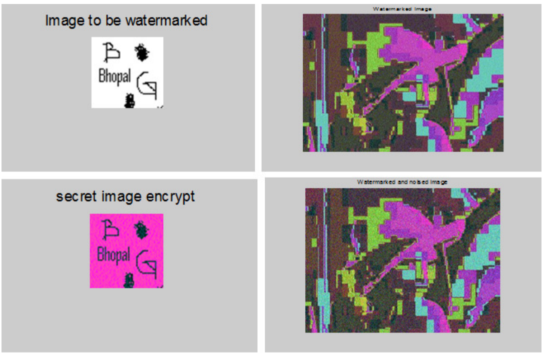


Fig. 6. Watermark image and encrypted images.

The figure shown below is the extraction process where the extraction of watermarked image is to be done. The figure shows the extracted watermarked image and decompressed image and the decrypted image respectively.

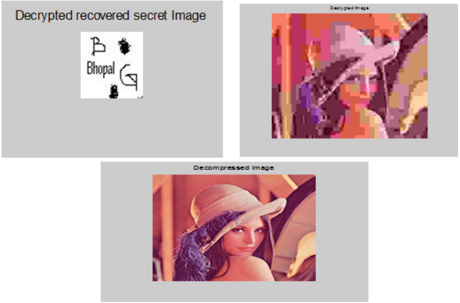


Fig. 7. a) extracted image b) decompressed image c) decrypted image.

A. Result Alanysis

The table shown below is the analysis of various encoding algorithm used for the compressin of images. The analysis is done on the basis of various parameters such as Peak Signal to Noise Ratio and CPU Time for various lossless compression algorithm. The experimental results are performed on Standard Lena image and shows that JPEG encoding has better PSNR and Comparatively low CPU Time.

Table 1 Analysis of Various Encoding Techniques on Lena Image.

Algorithm	PSNR Value on Women Image	CPU Time	
		Encoding	Decoding
JPEG	42.98	0.9 sec	0.9 sec
Wavelet	35.14	1.23 sec	1.08 sec
VQ	28.16	3.87 sec	3.95 sec
Fractal	27.45	6.84 sec	7.65 sec

The table shown below is the analysis of various encoding algorithm used for the compressin of images. The analysis is done on the basis of various parameters such as Peak Signal to Noise Ratio and CPU Time for various lossless compression algorithm. The experimental results are performed on Standard Women image and shows that JPEG encoding has better PSNR and Comparatively low CPU Time.

Table 2: Analysis of Various Encoding Techniques on Women Image.

Algorithm	PSNR Value on Lena Image	CPU Time	
		Encoding	Decoding
JPEG	33.38	0.11 sec	0.11 sec
Wavelet	30.56	0.32 sec	0.24 sec
VQ	27.14	2.37 sec	0.15 sec
Fractal	27.03	5.51 sec	1.28 sec

The table shown below is the analysis of various encoding algorithm used for the compressin of images. The analysis is done on the basis of various parameters such as Peak Signal to Noise Ratio and CPU Time for various lossless compression algorithm. The experimental results are performed on Standard Satellite image and shows that JPEG encoding has better PSNR and Comparatively low CPU Time.

Table 3: Analysis of Various Encoding Techniques on Satellite Image.

Algorithm	PSNR Value on Satellite Image	CPU Time	
		Encoding	Decoding
JPEG	56.48	0.5 sec	0.5 sec
Wavelet	42.64	0.9 sec	1.45 sec
VQ	31.43	4.85 sec	4.12 sec
Fractal	28.79	5.46 sec	5.43 sec

The figure shown below is the anlysis and comparison of various encoding technique. The analysis done here is on the basis of various images for the computation of Peak Signal to Noise Ratio. Here 3 standard images are taken i.e. Lena, Women and Satellite. The Peak Signal to Noise Ratio is then Computed for the given image. The experimental results shows that the Peak Signal Ratio is better for JPEG- Lossless encoding Technique.

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression).

$$PSNR = 10.log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

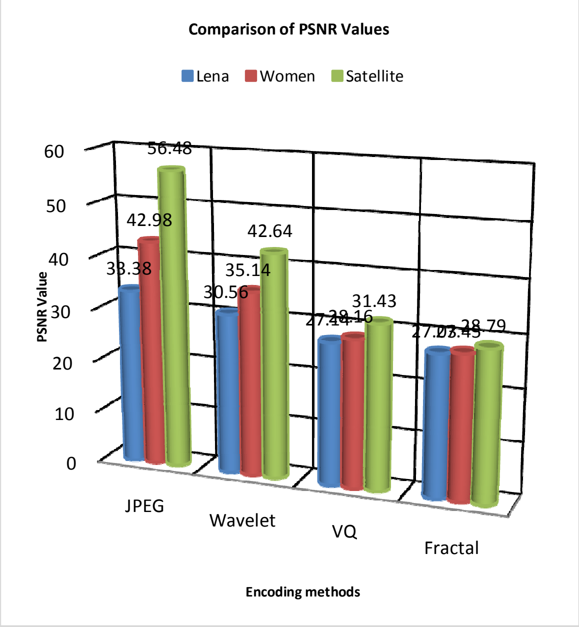


Fig. 8. Comparison of PNSR for various Encoding Techniques.

The figure shown below is the anlysis and comparison of various encoding technique. The analysis done here is on the basis of various images for the computation of CPU Time. Here 3 standard images are taken i.e. Lena, Women and Satellite. CPU Time is then Computed for the given image. The experimental results shows that the CPU Time is less for JPEG- Lossless encoding Technique.

CPU time (or process **time**) is the sum of **time** for which a central processing unit (**CPU**) was used for processing instructions of a computer program, as opposed to, for example, waiting for input/output (I/O) operations or entering low-power (inactive) mode.

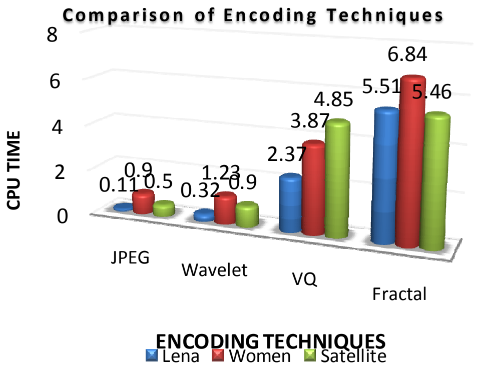


Fig. 9. Comparison of CPU Time for various Encoding Techniques.

The table 7 shown below is the analysis and comparison of various encryption techniques. The analysis is done on the basis of various parameters such as Key length and Rounds performed and Block Size and attacks possible.

The table show below is the result analysis of the proposed methodology implemented here for the watermarking. The results are tested for various images for various parameters such as No. of Colors and Mean Square Error and Normalized Cross Co-relation and Normalized Absolute Error.

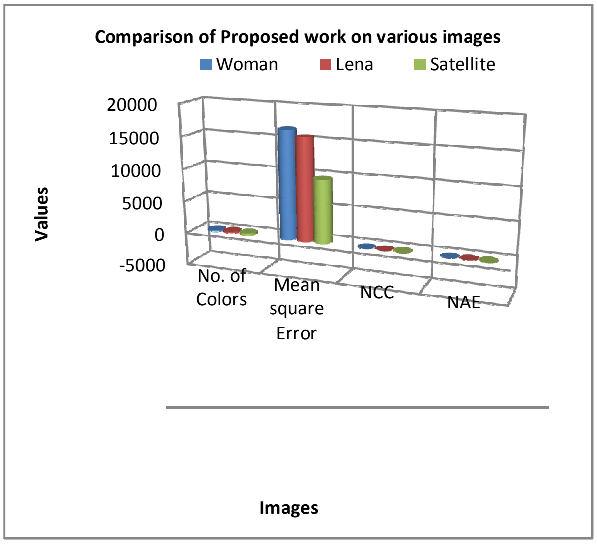


Fig. 10. Result Analysis of Proposed Methodology for Various Images.

The table show below is the result analysis and comparison of the proposed methodology on various parameters for different images.

Table 4. Analysis of proposed work.

Image	No. of Colors	Mean square Error	NCC	NAE
Woman	254	1.6640e+004	4.3038e-004	1.0005
Lena	239	1.5703e+004	7.2774e-004	1.0004
Satellite	256	9.6603e+003	-0.0016	1.0042

The figure shown below is the analysis and comparison of quality parameter with respect to compression ratio.

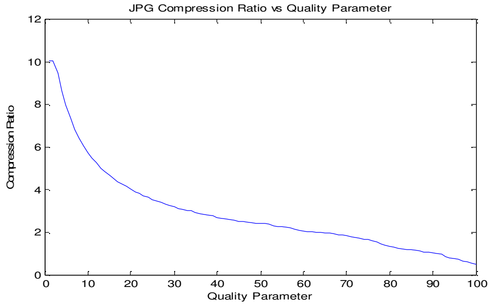


Fig. 11. Quality parameter vs compression ratio.

The table shown below is the analysis and comparison of existing and proposed work on the basis of CPU time and PSNR and payload capacity.

Table 5: Comparison of Existing & Proposed Work.

Parameters	Existing Work	Proposed Work
CPU Time	4.493	0.218
PSNR	34.151	59.79

The table shown below is the analysis and comparison of existing and proposed work on the basis of CPU time and PSNR and payload capacity.

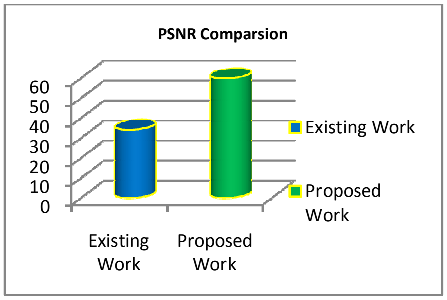


Fig. 12. Comparison PSNR.

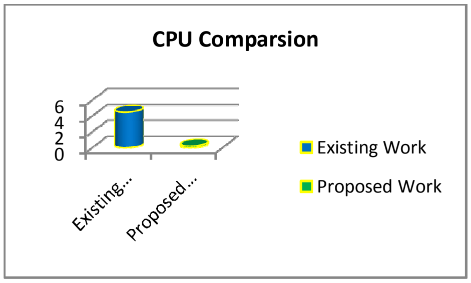


Fig. 13. Comparison CPU Time.

CONCLUSION

With algorithms that employ the Block Cipher and spread spectrum techniques in pressing watermark enables high performance. Deviations quality of the resulting image with embedded watermark when applied some of the analyzed techniques is satisfactory. Comparing the proposed methodology between existing method using performance metrics like MAE, NCC, NAE and PSNR to watermark. It can be concluded that they provide improved results than the existing method. The analysis of the simulation model provides that the implementation of an invisible watermark does not distort the image quality, taking into account obtained results for PSNR as an objective measure for the image quality which is about 31% more than the existing method. We also apply the security algorithm which makes our images more secure from the various forms of attacks.

REFERENCES

[1]. J. Sang and M. S. Alam, (2008). "Fragility and robustness of binary-phase-onlyfilter- based fragile/semifragile digital image watermarking," *IEEE Trans. Instrum. Meas.*, vol. **57**, no. 3, pp. 595–606, Mar. 2008.

[2]. H.T. Wu and Y.M. Cheung, (2010). "Reversible watermarking by modulation and security enhancement," *IEEE Trans. Instrum. Meas.*, vol. **59**, no. 1, pp. 221–228, Jan. 2010.

[3]. Samcovic, J. Turan, (2008). "Attacks on digital wavelet image watermarks", *Journal of Electrical Engineering,* Vol. **59**, No. 3, pp 131-138, 2008.

[4]. Y.Q. Shi, H. Sun, (2008). "Image and video compression for multimedia engineering: fundamentals, algorithms and standards", Taylor & Francis Group, 2008.

[5]. K. Hameed, A. Mumtaz, S.A.M. Gilani, (2006). "Digital image watermarking in the wavelet transform domain", *World Academy of Science, Engineering and Technology*, Vol. 13, pp 86-89, 2006.

[6]. K. Chawla, S. Singh, (2012). "Comparative analysis of watermarking techniques using frequency domain and wavelet domain technologies", *International Journal of Computational Engineering & Management,* Vol. **15**, No. 5, pp 74-76, 2012.

[7]. Deepti Shukla, Nirupama Tiwari and Deepika Dubey (2016). "Survey on Digital Watermarking Techniques", *International Journal of Signal Processing, Image Processing and Pattern Recognition,* Vol. **9**, No.1 (2016), pp.239-244.

[8]. Vineet Raj Singh Kushwah, Sumit Tiwari, Manvendra Gautam (2016). "A Review Study on Digital Watermarking Techniques" *International Journal of Current Engineering And Scientific Research (IJCESR)* ISSN (Print): 2393-8374, (Online): 2394-0697, Volume **3**, Issue 1, 2016.

[9]. R. Kaur, and S. Jindal, (2014). "Robust digital watermarking in high frequency band using median filter function based on DWT-SVD," *International Conference Advanced Computing and Communication Technology*, pp. 47-52, Feb 2014.

[10]. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich and T. Kalker, (2008). "Digital watermarking and steganography," San Mateo, CA, USA: Morgan Kaufmann, 2008.

[11]. E. Nezhadarya, Z. J. Wang, R. K. Ward, (2011). "Robust image watermarking based on multiscale gradient direction quantization, " *IEEE Trans. Image Process.,* vol. **6**, no. 4, pp. 1200-1213, 2011.

[12]. Potdar V.M., Han, S., Chang, E.; (2005). "A survey of digital image watermarking techniques", Industrial Informatics, 2005. INDIN '05. 2005 3rd IEEE International Conference, Page(s): 709 – 716, 10-12 Aug 2005.

[13]. http://homes.ieu.edu.tr/hozcan/EEE281/Intro_R2012b.pdf