MAT JOURNALS
Journal of Analog and Digital Communications
Volume 4 Issue 2

Blind Digital Watermarking System Using 2D-Dct

[1]Dr. Gayathri S, [2]Varsha R
Department of E&C, Sri Jayachamarajendra College of Engineering, Mysuru, Karnataka
Email id: *[1]sgmurthy_65@sjce.ac.in, [2]varshagowda9@gmail.com*

Abstract
In digital network systems the digital documents can be replicated and pass on effortlessly to extensive individuals with ease and free of cost. Multimedia data like image, video and audio files can be easily downloaded by public and they can easily manipulates. The approved proof as a steady and robust watermark should have been embedded in the digital pictures. The proposed work aims at developing a robust digital watermarking system, it incorporates an effective watermarking algorithm which solves the above problem. New blind frequency watermarking algorithm using 2-Dimensional Discrete Cosine Transform and 1-Dimensional Walsh vectors has been proposed.

Keywords: *Robust, Embed, Algorithm, 2D-DCT, Multimedia, Watermark*

INTRODUCTION

Watermarking is known as activity of concealing a message, logo, text or signature into a picture, video file or any other work of media in a way that the crumbling of quality is reduced and stay at an imperceptible level. Numerous digital watermarking algorithms have been proposed in frequency domain i.e. spatial and transform domains.

The techniques used in spatial domain still have comparably low bit capacity and are vulnerable to lossy image compression and other image processing operations .The common frequency transforms such as Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DWT) are used for watermarking in the frequency domain.

Watermarking algorithms embed digital data or signature to prove the owner's integrity and to stop copyright infringement. For the copyright protection, the algorithm should be blind.

The original media is not required to remove the watermarking data in daze strategy. Security turns into a vital issue which requires the watermark to be changed just by the proprietor.

RELATED WORK

Embedding of watermark to the middle frequency coefficients of grey scale digital image is proposed in [1]. Zigzag distribution of coefficients and the blind method, where original image is not needed to extract the watermark is included in this paper. Result shows that this algorithm is robust to attacks like filtering, JPEG compression and some signal processing operations.

A new embedding strategy based on quantitative analysis of DCT coefficient magnitudes of a gray scale image using series of 8×8 DCT matrices [2] is discussed. They petitioned that the implemented algorithm provides more robust when watermarks are embedded in a DC components, which has more perceptual capacity compared to AC components.

Using spatial masking method, an adoptive watermarking algorithm was developed. In this method DCT blocks are classified into two categories: strong and weak textures. Correlation techniques are used in the process of extraction.

Embedding of watermarked data in frequency coefficients such as low and

high frequency DCT components is proposed in [3]. A grey scale image which is of 512×512 is divided into two parts, central and small parts which represent rest of the image. Effect of cropping attacks is reduced. This algorithm is more robust to various attacks.

A new watermark embedding algorithm was introduced in [4] where 8×8 blocks of DCT are used to select some of the AC components of DCT blocks for embedding watermark using some quantization and modulus calculations.

The algorithm is blind and extraction of watermarks without original image is achieved. To identify the existence of watermark, correlation between original and extracted watermark is calculated. Empirical result shows that the proposed method is more robust to JPEG compression.

Digital watermarking scheme using color images for embedding watermark in the DCT domain for copyright protection is proposed in [5]. In this algorithm the color image is converted to YCbCr form first.

The embedding method is achieved by inserting the binary watermark into the DCT coefficient of the Cb and Cr components according to their numerical status (0 or 1). It utilizes the middle and high frequency components for modification.

The implemented algorithm is blind and the extraction is implemented without resorting to the original image. The method has been tested against signal processing operations and proved to be robust.

Based on the chaotic Direct Sequence Spread Spectrum (DSSS), a new multi-bit watermarking scheme in the DCT domain which is combined with error correcting codes (ECC) and a Human Visual System (HVS) model in the spatial domain is discussed in [6].

It uses 256 × 256 grey level host image is divided into 8 × 8 blocks. In this scheme scaling factor is used to improve robustness. 27 low frequency locations are used from each block by modifying the DCT coefficients. In the extraction the original image needed, as the scheme uses the same noise signals that are used in embedding for correlation.

This means that the embedded data can be recovered as follow: if the correlation is positive, the embedded data is 1, and if the correlation is negative, the embedded data is -1. The proposed scheme uses BCH code to improve robustness and also shuffling to enhance security.

The robustness of the algorithm has been tested with StirMark 4.0. The algorithm is blind and the 64 bit watermark was retrieved without the original image during the decoding process. This method has been tested against many attacks including JPEG compression and some common signal processing attacks.

A robust watermarking based on the DCT is discussed in [7]. It uses 512 × 512 host image for embedding watermark into an image. The algorithm selected certain DCT values for modification to achieve the embedding of a binary watermark into the image. Before embedding, the algorithm scrambles the binary watermark data to increase security and robustness.

Then a pseudo random number generator and a secret key are used to select an AC coefficient from locations in the DCT. The average moment of the neighboring coefficients around that position is then computed to modify this AC value. IDCT is then taken to generate the watermarked image.
In the extraction process, the watermarked image is segmented to 8 × 8 blocks and applying the DCT, later reverse procedure is implemented. Different attacks were used such as sharpening, blurring, noise, cropping, rotation, scaling and JPEG compression.

Walsh Hadamard Matrix is used for embedding the watermark is proposed in [8]. The original image is DCT transformed. The Walsh code is used to implement the correlation as a measure of the similarity between extracted watermark and original embedded watermark in the image.

The watermarked image is shifted 1 pixel in the vertical direction and 1 pixel in the horizontal direction. The original watermarked and shifted watermarked images are then used as inputs into the detection process. The method is blind and the original image is not required for detecting.

An algorithm that exploits Complex Hadamard Transform (CHT) for embedding watermarks in digital images is proposed in [9]. An image with pixel size 100 × 100 was used as a watermark to be embedded in a 512 × 512 cover image, exploiting the low frequency area. The technique is blind and doesn't require the original image in the extraction.

A digital watermarking algorithm based on DCT domain and 2D Hadamard Transform is discussed in [10]. In the scheme the cover image undergoes permuted before it is divided into blocks and then DCT is applied. 64 × 64 watermark is coded by 2D Hadamard Transform and then the DCT coefficients are selected for embedding.

The watermarked image is obtained by applying the IDCT and inverse the permutation. The presented scheme uses a grey scale image of size 512 × 512. The NC is utilized for verifying the quality of the extracted watermarks. PSNR is also applied to compare the similarities between the original and the watermarked images. The resulted PSNR value ranges from 36.5 dB to 42.2 dB.

METHODOLOGY

The proposed watermarking system includes watermark embedding and extraction processors with verification module block diagrams.

As shown in Figure 1 digital watermarking system consists of watermark embedding processor, communication channel through which data will be transferred and a watermark extraction module, that extracts the watermark from the data.

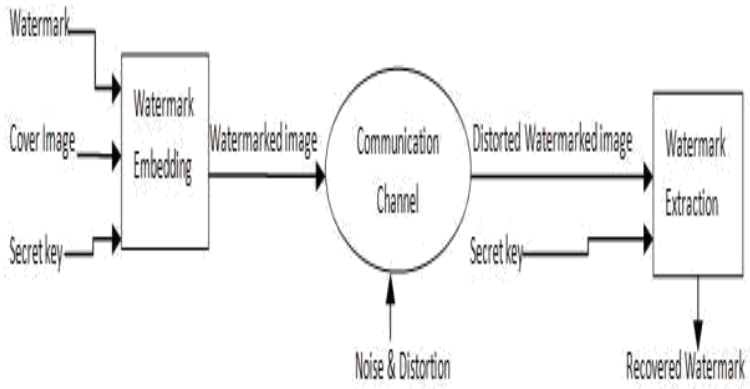

Fig 1: *Digital watermarking system*

Watermark Embedding Processor

It embeds the watermark to the image by making use of blocks as shown in Figure 2. It includes DCT and IDCT modules, watermark embedding module.

DCT Block

This block performs DCT of a cover image. Output of DCT block is then applied to watermark embedding module.

Watermark Embedding module:
This module embeds encoded watermarks to the DCT coefficients. The output is then applied to IDCT module.

2D-IDCT
Once the Watermark is embedded, coefficients are then fed to IDCT to convert frequency coefficients to spatial values.

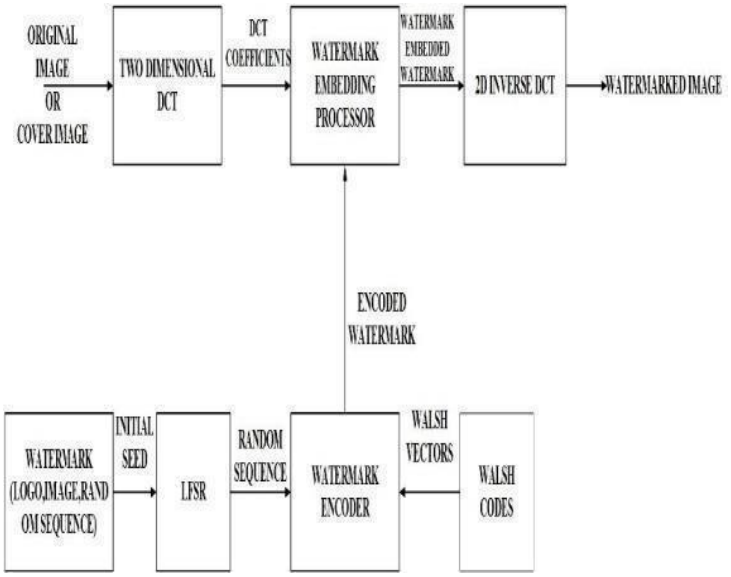

Fig 2: *Watermark embedding processor*

Watermark Encoder
It encodes watermark generated using LFSR with the Walsh codes, to provide security to the watermark. It includes LFSR and Walsh buffer.

Watermark Extraction and Detection Processor:
It extracts the watermark from the watermarked cover image with the help of blocks as shown in Figure 3

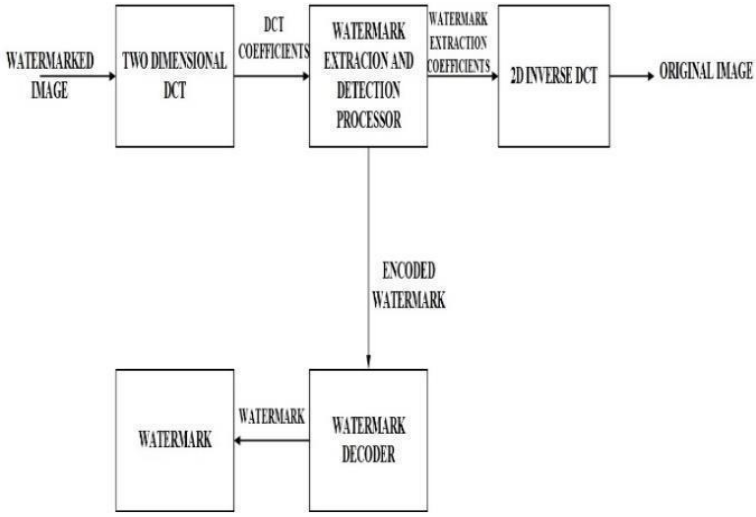

Fig 3: *Watermark extraction and detection processor*

Discrete Cosine Transform
Image is first transformed to its frequency domain using

2D-DCT. Since DCT is suitable for all image compression applications. Image in spatial domain is translated to its frequency representation using DCT. In general, compared to high frequency coefficients in an image, lower frequencies are more dominate in nature.

In Frequency domain, Using DCT, high frequency components can be removed without affecting too much image quality. There are three frequency components in DCT: low, middle and high frequency components. Watermarks are embedded into any one of the component or combination of frequency components in watermarking techniques.

In the proposed method, watermarks are embedded into low frequency components and high frequency components are neglected, since human visual system is more sensitive to low frequency components rather than high frequency components. Using a series of 1D-DCT, 2D-DCT coefficients are calculated. Figure 1 depicts the basic block diagram of watermarking system.

Walsh Vectors

Walsh codes are termed as Walsh vectors which are orthogonal and include length elements. It incorporates a series of square pulses with a value +1 & -1. Walsh sequence comprises of code of lengths of k=2n, n represents an integer. By using code length of k, K number of orthogonal codes can be obtained. Based on the length of Walsh sequence, number of functions can be produced. Walsh sequence can be acquired by numerous procedures, however best strategy to get Walsh codes is manipulating Hadamard matrices. The order of Hadamard matrices are in terms of power of two. Even when the image is distracted, watermarks can be extracted using Walsh codes because of its correlation property.

For the proposed method Walsh codes play an important role since it is going to detect the tampered pixel values. Using Walsh codes, whether image is tampered or not can be detected. Watermarks are encoded with Walsh codes using Walsh encoder.

Figure 2 and Figure 3 depicts the block diagram of both embedding and extraction processor.

Watermark extraction and detection processor is used to extract the watermark which is embedded in an image. It also consists of DCT block, IDCT block same as embedding processor part. It also consists of watermark decoder to decode the watermark and extraction and detection processor.

DCT Block

This block is same as the DCT block used at source part or embedding part. But the input is watermarked image. Output of DCT block is then applied to watermark extraction and detection block.

2D-IDCT

Once the Watermark is extracted, coefficients are then fed to IDCT to convert frequency coefficients to spatial values. Operation is same as the IDCT block in embedding processor.

IMPLEMENTATION

Implementation of digital watermarking system is done using matlab and Verilog complier. Watermark is embedded and extracted from an image using the algorithm. Flow of the watermarking system is explained in the following modules using the flow charts as shown in Figure 4, Figure 5 and Figure 6.

Watermark Embedding Process

1. Consider 128 × 128 matrix
2. Divide entire matrix into 8×8 sub blocks and apply 2D-DCT to each block
3. Using a secret key which is of 16 bits is applied as a initial seed to the lfsr. Consider only 16 sequences each of 16 bits and those 16 sequences are encoded with walsh codes.
4. Encoding procedure: Consider walsh codes of 8 vectors and also divide 16 bit sequence of lfsr to two half i.e. 8,8 and then multiply each 8 bit sequence with 8 vectors of walsh codes. Each bit in sequence is multiplied with each vector.
5. Each bit in encoder is embedded into each 8×8 dct block. In particular, 4 low

frequency coefficients should be considered.

6. Embedding is done by rounding off each coefficient values mentioned above to even or odd. Here double precision coefficients are considered, which improves the Signal to Noise Ratio (PSNR).

Rounding to even:

dct_even = 2 * round (dct_coeff / 2)……..(1)

Rounding to odd:

dct_odd = 2 * round ((dct_coeff + 1) / 2)...(2)

If encoded bit is 0 then coefficient is rounded to even, If 1 then rounding into 1 as shown in equation (1) and equation (2)

Once this is done for entire 8×8 matrices Inverse DCT is applied.

Figure 4 depicts the flow chart of watermark embedding process.

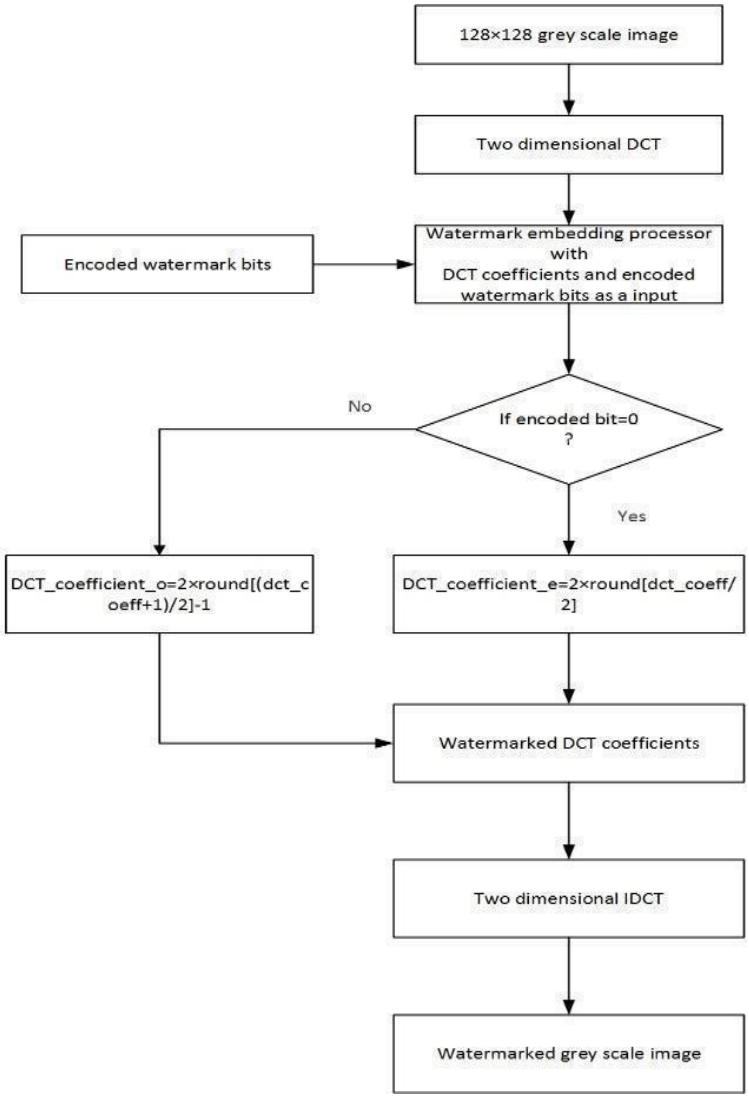

Fig 4: *Watermark embedding process*

Watermark Extraction and Detection Part:

In this block, watermark will be extracted from DCT coefficients. Algorithm behind extraction of watermark is

1. Consider the DCT coefficients to which watermark bit has been embedded. If the coefficient value is even then 0 will be extracted else 1 will be extracted.

2. Continue the procedure for all 8×8 DCT blocks to extract complete encoded watermark. For example if the coefficient value is 0.036 then 0 will be extracted as a watermark bit else if the coefficient value is 0.975 then 1 will be extracted.
3. Once all the encoded watermark bits extracted, they are subjected to watermark decoder to separate Walsh codes and random sequence

Figure 5 depicts the flowchart of watermark extraction process.

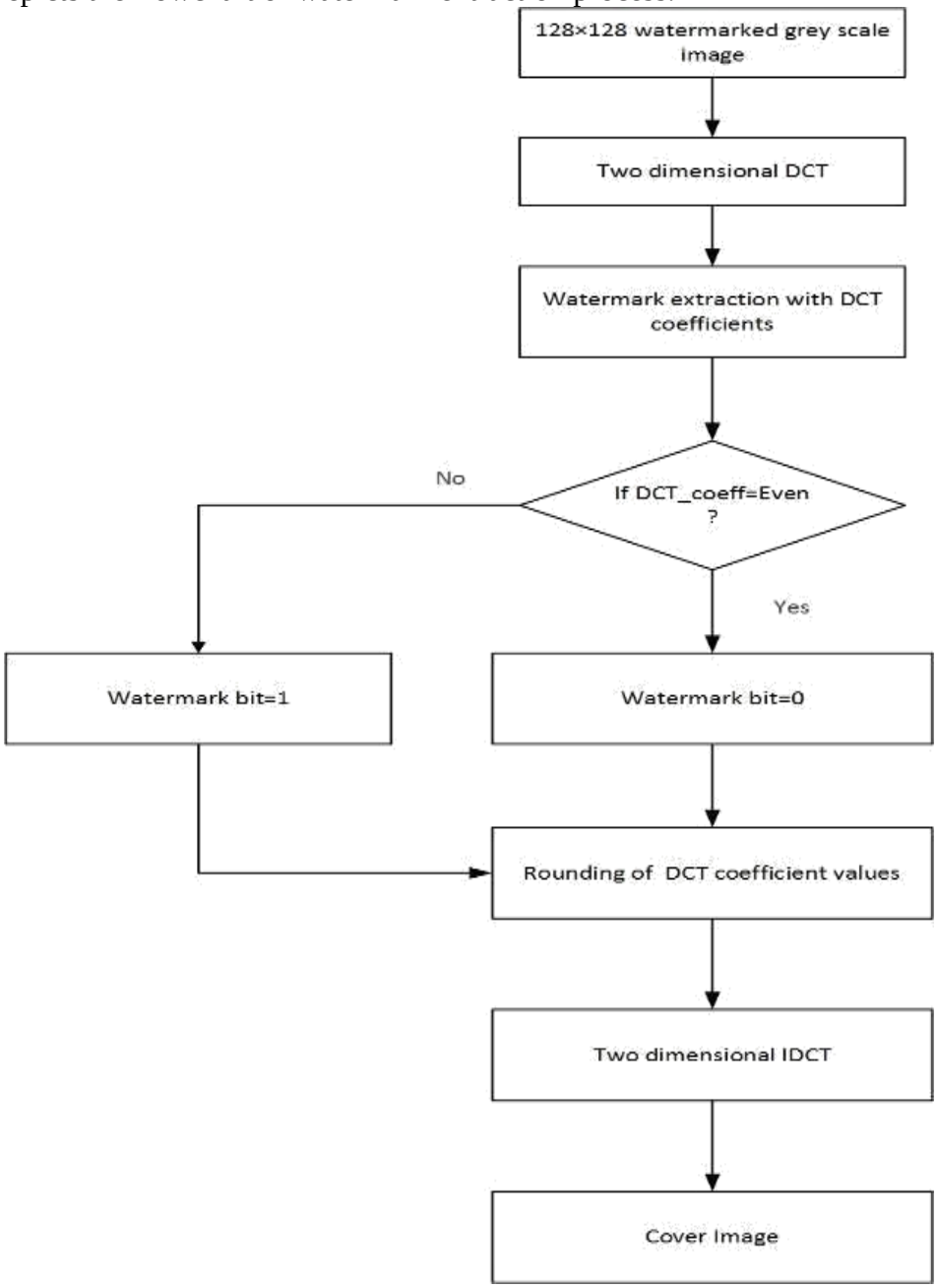

Fig 5: *Watermark extraction process*

Verification

Verification of watermark is done by the following steps:

1. Extracted watermark from watermarked image and obtained watermarked from secret key are fed as an input to the comparator.
2. If the comparator output is 1 then authentication is done and Tampering=0. I.e. no tampering is done on the image, since comparator compares each bit of both watermarks.
3. If the comparator output=0 then authentication would be fail and shows the bit positions where mismatch is occurred. For source detection application, using the obtained error codes, device from which tampering is done could be detected since code indicates the device identity number and acknowledge the original source to resend the data.

Figure 6 depicts the verification process of extracted and derived watermarks. For ownership application, extracted watermark could be shown as a proof, algorithm is only known to the creator. For tampering detection application, results of proposed system can be used to detect where exactly tampering is done. It shows the bit positions where the bit values are altered.

RESULTS

Proposed design is simulated in Matlab. Input image is embedded with watermark in the watermark embedding module. It is extracted and verified at the extraction and detection module. If the derived and extracted watermarks matches in the verification module, then the pop up window appears with the authentication and tampering detection with the bit mismatch along with bit position and it displays secret key of a source device as shown in Figure 7.

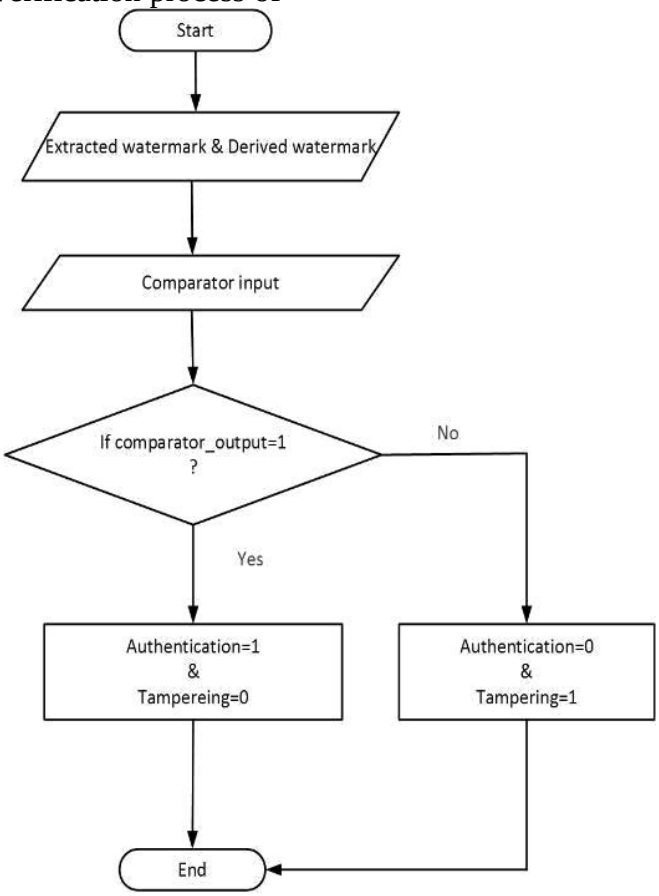

Fig 6: *Verification process*

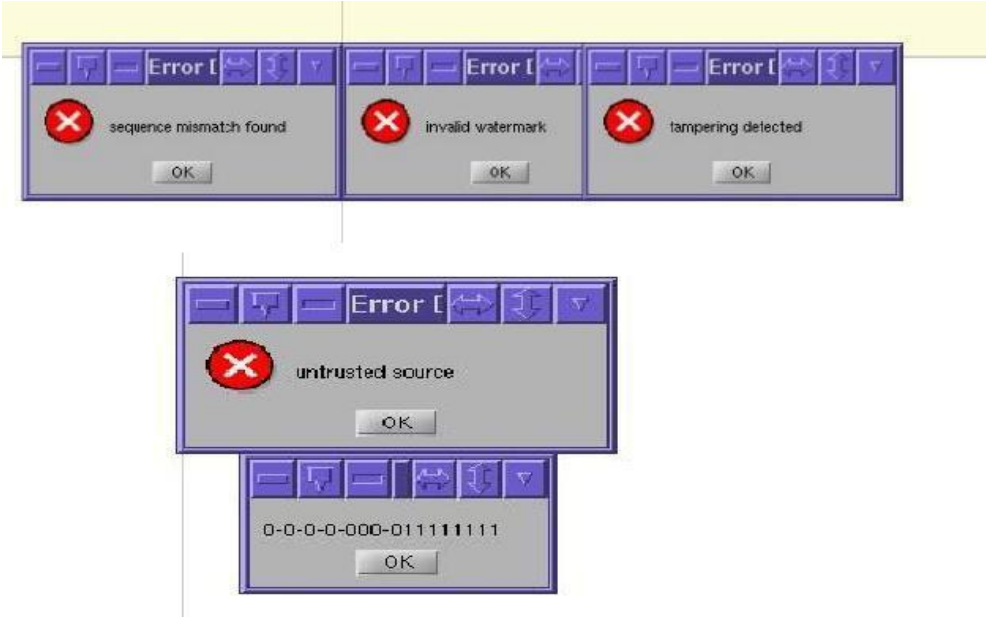

Fig 7: *Invalid watermark*

When both the watermark matches then the same pop up with authentication match with source code will be displayed as shown in Figure 8.

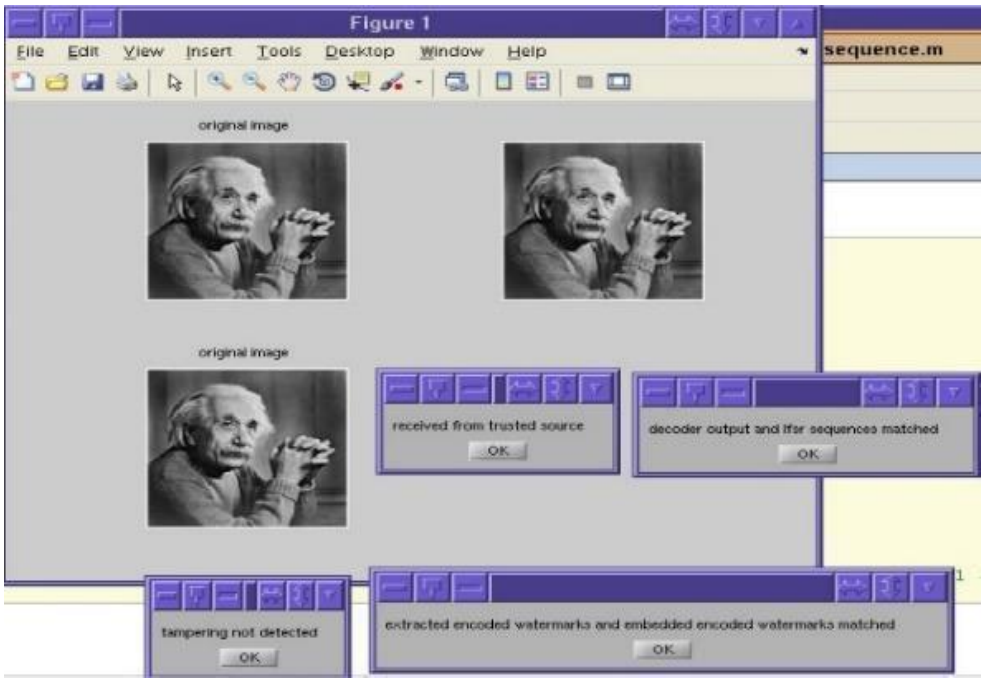

Fig 8: *Matlab results*

Peak Signal to Noise Ratio is a quality measure parameter which assures quality of the watermarked image with respect to original image. It is calculated for watermarked image with respect to input image to find out the distortion introduced after inserting watermark.

It is expressed in dB. More the PSNR value, more will be the correlation between two images.

Table 1: *PSNR value of input images*

Watermarked Image	PSNR with normal algorithm(dB)	PSNR value with proposed algorithm(dB)
Einstein Image	105.9278	125.0233
Monalisa	104.9344	124.9835
Internet	104.2133	124.8656
Cameraman	105.4979	125.0069
Lena	103.6079	124.5830

The PSNR value for some images is recorded as shown in Table 1. The proposed system performance in terms of PSNR is validated with the normal algorithm.

Compared to normal watermarking systems, the proposed system generates watermark images that have high PSNR values. Hence image distortion is very less in this proposed system compared to normal algorithms.

CONCLUSION

The proposed digital system provides several features such as authentication, tampering detection, source detection and ownership proof. It can quickly detect tampers on an image and authentication process is more robust. With this feature it is cumbersome to copy data as well as to destroy the watermark.

It includes proper authentication algorithm. Hence the data will be received or stored only when it is sent from trusted source, otherwise data will be removed and acknowledge the required source to resend the data.

Thus the proposed system offers better perceptual performance aspect of the watermarked image. It boosts the security feature for attacks like compression and rotation. It is more robust to various attacks compared to other implemented digital watermarking system.

REFERENCES

1. M. Barni, F. Bartolini, V. Cappellini, A. Piva,"Robust watermarking of still images for copyright protection", published in IEEE Digital Signal Processing Proceedings, Vol.2, pp. 499-502, 1997
2. J Huang, Y Q Shi, Y Shi, "Embedding watermarks in DC components", published in IEEE Transactions on Circuits and Systems for Video Technology, Vol.10, pp.974-979, 2000.
3. F. Alturki and R. Mersereau, "Robust oblivious digital watermarking images using DCT phase modulation, presented in IEEE International Conference on Image Processing, Vol.2, pp.84-87, 2000
4. Y Jang, I Kim, H Kang, K Kim, Seung-Soo Han, "Blind digital watermarking Algorithm Using Complex Block Selection Method", published in Springer, pp.996-1001, Berlin, 2001,
5. Z. Jiang-bin, Z. Yan-Ning, F. Da-gan,

Z. Rong-chun, "Colour Image watermarking Based on DCT-Domains of Colour Channels", IEEE Conference on Computers, Communications, Control and Power Engineering, Vol.1, pp.281-284, TENCON, 2002

6. X Li, X Xue, W Li, "An Optimized Multi-Bits Blind Watermarking Scheme", Springer, pp.360-369, 2003.
7. Wen-Chuan Wu, Guang-Ruei Ren, "A DCT-Based Robust Image Watermarking Using Local Moment" Presented in IEEE International Conference on Data Mining and Intelligent Information Technology Applications, pp.122-126, 2011.
8. A. U Sakova, J. Kotuliakova, "Using of WHT in the Detection Process of the Watermarking Systems", presented in IEEE Conference on Video/Image Processing & Multimedia Communications, VIPMC, Vol.2, pp.727-732, Croatia, 2003
9. R. Kountchev, S. Rubin, M. Milanova, V. Todorov, R. Kountcheva, "Resistant Image Watermarking in the Phases of the Complex Hadamard Transform Coefficients", presented in IEEE International Conference on information Reuse and Integration, pp.159-164, 2010
10. J. Wassermann, A. Dziech, "New Robust Watermarking Embedding Scheme based on Combination of Basis Images of 2D Hadamard ransform and Quantization Index Modulation" Recent Researches in Computers and Communications, pp78-82.