ROBUST AUTHENTICATION OF JPEG IMAGES USING DCT BASED WATERMARKING AND GENETIC ALGORITHM

Dinesh Yadav
M.Tech. Scholar, Department of Computer Science and Engineering
Rajasthan Institute of Engineering and Technology, Jaipur
Dr. Sachin Sharma,
Professor, Department of Computer Science and Engineering
Rajasthan Institute of Engineering and Technology, Jaipur
Mr. Amit Bairwa,
Asst. Professor, Department of Computer Science and Engineering
Rajasthan Institute of Engineering and Technology, Jaipur

***Abstract*— One of the most popular formats for image storage is JPEG/JPG. It stands for Joint Photographic Expert Group format. It uses Discrete Cosine Transform over non-overlapping blocks of image pixel matrix for image compression and storage. JPEG provides a high degree of compression as compared to other image formats. In modern scenario, authentication is becoming a prime concern with digital data meant to be distributed over the internet or otherwise. A large number of jpeg images are shared everyday over internet, or other media, with a substantial fraction comprising of those in which authentication is critical. However, due to the advancements in technology and the computing capabilities, it is possible to modify an image for doctored content even with the cheapest commodity computer. This includes medical images, satellite images, surveillance camera images and images related to applications in which authenticity is the prime concern. In this Research Paper, a technique is proposed to authenticate JPEG images using LSB encoding in Discrete Cosine Transform Coefficients of the Group of Blocks (GOB) of the image. The contribution of this research work is two-fold. It suggests a method to embed watermark in JPEG image so that the watermark is compatible to the JPEG compression. Secondly, it uses Genetic Approach so as to maintain the statistical properties of the image so that it is difficult for an attacker to identify through statistical investigation on the pixel values of the images that weather the image is watermarked or not. It turns out that direct embedding of watermarking bit in the DCT coefficients results in considerable distortions in the cover image leading to visible distortion and high Mean Square Error, leading to low PSNR. The selection of GOB and the Coefficients is based on the Genetic Algorithm to yield the best PSNR so as to preserve the quality of the marked image. This work extends the technique proposed by Oh-Jin-Kwon et. al. [1] by making use of the Genetic Algorithm for the selection of coefficients and the GOB blocks. MATLAB is used as the simulation tool and the results obtained are compared with the benchmark techniques to establish the authenticity of the proposed technique.**

Keywords : Image Authentication, Watermarking, Discrete Cosine Transform, Genetic Algorithm, PSNR, MSE

I Introduction

1.1 Introduction

JPEG/ JPG refer to Joint Photographic Expert Group. This compression technique was developed by International Telecommunications Union (ITU) in its specification T.86 [2]. The main objective of the image compression techniques are:

1. To Store the Image in a compressed form
2. To enable efficient transmission of the Image in its compressed form.

JPEG compression is flexible in a way that it can be used to implement both lossy and lossless compression. However, the most commonly used JPEG technique for color images and JPEG compressed video transmission using Lossy techniques to reduce the size of the payload data. The same is discussed in this Research Paper.

1.2 Fundamentals of Lossy Compression

The JPEG image compression takes-in few simple steps to convert a raw image into compressed image. The compressed image can rendered (displayed) using a number of program including web browsers like Internet Explorer and Mozilla Firefox. In JPEG compression, the raw image is partitioned into blocks of 8X8 pixels as shown in figure 1.1 and 1.2.

Figure 1.1 Lena Image 180X180 Pixel

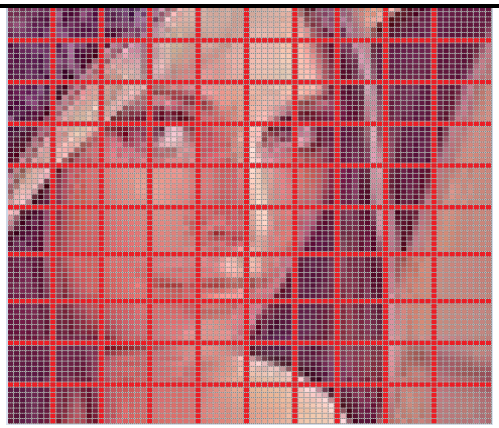


Figure 1.2 Lena Image 80X80 Pixel (Magnified 300 times)

The color scheme used in JPEG scheme is Y, Cb, Cr, where Y is the luminance parameter and Cb and Cr are Chrominance Parameters [3]; (specifically, Cb refers to chrominance w.r.t. Blue and Cr refers to Chrominance w.r.t. Red). The raw image consists of 3 color components; viz Red, Green and Blue, where each of the color component is specified by 8 bits having range from 0 to 255. For the sake of simplicity, assuming that only 8 bits are to be operated, let the pixel matrix is as shown in Equation 1.1.

TABLE 1.1

PIXEL MATRIX OF 8X8 PIXEL BLOCK

52	55	61	66	70	61	64	73
63	59	55	90	109	85	69	72
62	59	68	113	144	104	66	73
63	58	71	122	154	106	70	69
67	61	68	104	126	88	68	70
79	65	60	70	77	68	58	75
85	71	64	59	55	61	65	83
87	79	69	68	65	76	78	94

It is evident that the range of pixel values is from 0 to 255. For a simple compression technique based on DCT, we need to convert the range from 0 to 255 to -128 to 127. To do this, the straightforward way is to subtract 128 from each of the values. Doing so gives the matrix shown in table 1.2.

TABLE 1.2

PIXEL MATRIX OF 8X8 PIXEL BLOCK
(NORMALIZED VALUES FROM -128 TO 127)

-76	-106	-67	-62	-58	-67	-64	-55
-65	-69	-73	-38	-19	-43	-59	-56
-66	-69	-60	-15	16	-24	-62	-55
-65	-70	-57	-6	26	-22	-58	-59
-61	-67	-60	-24	-2	-40	-60	-58
-49	-63	-68	-58	-51	-60	-70	-53
-43	-57	-64	-69	-73	-67	-63	-45
-41	-49	-59	-60	-63	-52	-50	-34

The Discrete Cosine Transform helps in separating a given the image into parts known as spectral sub-bands [4], having differing importance to the image's visual quality. This is illustrated as shown in Figure 1.3.

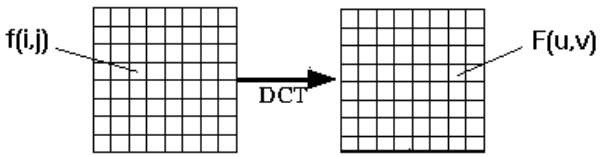


Figure 1.3 DCT Transformations from Spatial to Transform Domain.

The general equation of DCT Transformation of N data items is as follows:

$$f(u) = \left(\frac{2}{N}\right)^{1/2} \sum_{i=0}^{N-1} \Lambda(i) \cos\left[\frac{\pi . u}{2.N}(2i+1)\right] f(i)$$

Where

$$\Lambda(i) = \begin{cases} \frac{1}{2} & if\ i = 0 \\ 0, otherwise \end{cases}$$

The Two-level DCT Transform is straightforward on similar lines as one dimensional transform. The Two dimensional transform is explained in detail in Section 3. The advantage of DCT Transform is that for most of the images, much of the signal energy lies at low frequencies which appear in the upper left corner of the DCT. Let this matrix be called $A_{j.k}$.

The next step is the quantization using a variable quantization matrix $Q_{j.k}$. The JPEG compression follows a specific Quantization matrix as shown in the Table 1.3.

TABLE 1.3

QUANTIZATION MATRIX FOR JPEG IMAGE COMPRESSION

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

A resultant matrix is computed as follows:

$$B_{j.k} = \frac{A_{j.k}}{Q_{j.k}}$$

After pairwise division and rounding operation, the matrix so obtained is as follows:

TABLE 1.4

RESULTANT MATRXI AFTER DIVISION WITH QUANTIZATION MATRIX AND ROUNDING OFF

-26	-3	-6	2	2	0	0
0	-2	-4	1	1	0	0
-3	1	5	-1	-1	0	0
-4	1	2	-1	0	0	0
1	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

The zig-zag scan is performed until all zeros are obtained. Thus, only non-zero values need to be stored, and thus, JPEG compression is achieved. The above process is the key process which is used in both JPEG compression and mpeg video encoding of the video.

The Layout of this Research paper is as follows:

Section 1 presents an overview of the subject matter and gives the problem statement and the approach for the research. Section 2 provides the overview of Problem Statement and Motivation for this research work. Section 3 presents the

proposed model for watermarking of the image in transform domain. Section 4 gives the simulation results and the plots for various parameters related with quality metrics such as PSNR and MSE [7]. Section 5 concludes the Research Paper.

II PROBLEM STATEMENT, MOTIVATION AND RESEARCH APPROACH

The most important characteristics of an effective watermarking scheme for images should have the following features [5]:

1. The watermarking process should enable the determination whether an image has been altered or not.
2. The watermarking process should be able to locate any alteration which is made on the image.
3. The watermarking process must be able to integrate the authentication data with subject image rather than as a separate data file.
4. The watermarking process must be implemented in such a way so as to minimize the visual imperfections in the image.
5. The watermarking process is implemented in such a way that it will be able to detect even the slightest alteration with the image.

This Research Paper aims to devise a method for forgery detection in JPEG images in Transform Domain, i.e., the Discrete Cosine Transform Coefficients. The proposed technique is watermarked based, which means that it embeds watermarking bits into the image file for the purpose of tempering detection. It is observed in the benchmark approaches that embedding of watermarking bits directly in transform domain coefficients results in visual imperfections in the image. In this Research Paper, the approach is augmented with genetic algorithm so as to reduce the imperfections and provide better PSNR. The approach uses a Fitness Function which is repeatedly applied on a set of coefficient values, thereby assisting in the selection of best possible pixel pairs or Group of Blocks for the embedding process.

There are a large number of applications which requires authentication and authorization of the transmitted images [5]. A number of such applications include Surveillance Camera Images, Satellite Images, Medical imaging etc. With the increase in the image exchange over the internet and its distribution to stakeholders over open networks, the possible threats of image manipulation has been increased drastically. Thus, there is a need for a watermarking scheme that will detect the tempering (if any) in the image. Moreover, as most of the images are transmitted in JPEG compression format, it is more useful to investigate a watermarking scheme applicable to JPEG images.

The image watermarking model presented in this Research Paper is applicable over the process through which the raw image is compressed and stored in JPEG format. The compressed image holds the watermark which is invisible. The watermark is embedded in the high frequency DCT coefficients which are obtained after the operation of image matrix with the quantization matrix. Resistance to Statistical attacks with better Image quality is maintained using Genetic Algorithms [6]. Thus this watermarking scheme is robust against JPEG compression. If some tempering is done on the host image, then the values of the corresponding DCT Coefficients gets changed resulting in the detection of tempering at the receiver. This process in implemented through an algorithm which runs at the receiver end to render and authenticate the received image.

III .PROPOSED WORK

3.1 JPEG Image Compression

The Joint Photographic Experts Group developed the, now most popular, JPEG algorithm in the year 1992. It was developed to address the issues of that era, most importantly, the facility that commodity computers have enough processing capabilities to manipulate and display full color photographs. Nevertheless, a full color photograph required tremendous amount of bandwidth when required to be transmitted over a network. This is clear with the following illustration.

Consider an image of 800X900 pixels with each pixel represented by three color components; viz; Red, Green and Blue and each color is specified using 8 bits. Thus, the number of bits required to specify a single pixel is 24 bits, or 3 bytes. The total number of bits repressing image file is thus, 800X900X24 = 17280000 bits or about 16 Mb. Such an image can be significantly compressed using suitable compression technique so as to enable it to be stored and transmitted efficiently.

The basics of any compression technique lies in the removal of redundant information from the image and to store the information which is required to suitably render the image with acceptable quality. The compression techniques which were available before JPEG had major drawbacks. They support very low amounts of compression and major data loss during the image compression, resulting in visual imperfections. The JPEG algorithm was developed aiming at high compression of images with minimal data loss and high compression ratios.

The term “Photograph” is used for an image taken from a camera. It is a natural image having certain particular statistical pattern and associated redundancy. On the other hand, the term “Image” is used in a broader sense to include photographs as well as artificial images obtained as a result of image operations through image editors such as Adobe Photoshop etc. Such images do not have natural statistical properties and are often accompanied by sharp edges and color borders.

Due to the mathematical basics of the compression technique, JPEG is excellent at compressing color photographs and gray-scale photos that include 256 (0 to 255 integer values) shades ranging from black (i.e. 0) to white (i.e. 255). However, the JPEG algorithm does not work well with layered graphics, clip art, text, or images with sharp transitions at the edges of objects.

JPEG compression and decompression consist of 4 distinct and independent phases:

1. First, the image is divided into 8 x 8 pixel blocks.
2. A Discrete Cosine Transform is applied to each block to convert the information from the spatial domain to the frequency domain. This transform is used as it localizes the information contained in the block to few coefficients located at the top right corner of the matrix.
3. The frequency information is quantized using Quantization matrix to remove unnecessary information.
4. Finally, Standard compression techniques are applied to compress the final bit stream as per the JPEG format.

3.2 Watermarking of JPEG Images

The Proposed technique aims to implement a mechanism so that a custom watermark is suitably embedded in an image. This watermark is embedded in DCT coefficients used for JPEG compression. This watermarking scheme will be fragile and therefore, the watermark will be lost even with slight tempering of the image, thereby, providing a mechanism for

detection of image forgery. As the watermark is embedded in DCT coefficients, the JPEG compressed image carries the watermark. However, to control the visual imperfections in the image as a result of manipulation of the DCT coefficients, Genetic Approach is used to suitably modify the other bit planes so that MSE and PSNR can be kept within acceptable thresholds. The proposed model is illustrated in the figure 3.1.

JPEG uses luminance/chrominance (Y Cb Cr) color space as opposed to the RGB color space used in Raw Images. The following system of equations is used for converting between the two color spaces:

$$\begin{cases} Y &= 0.1818R + 0.612G + 0.06168B + 16 \\ Cb &= -0.1006R - 0.3299G + 0.4375B + 128 \\ Cr &= 0.4375R - 0.3973G - 0.04025B + 128, \end{cases}$$
$$where \;\; 0 \le R, G, B, Y, Cb, Cr \le 255 .$$

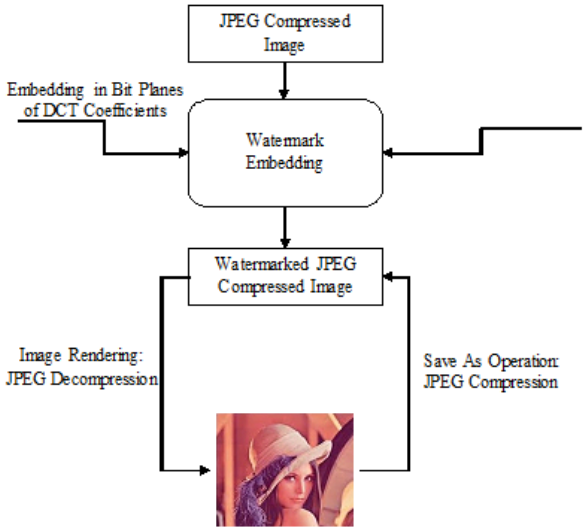


Fig 3.1 Generic Watermarking Scheme

The proposed technique of watermarking of JPEG format is shown in the figure 3.1. In JPEG compression, the raw image in RGB color format is converted to Y, Cb and Cr format. Each of the Color plane Y, Cb and Cr is partitioned into 8X8 pixel blocks. The compression can be achieved at this stage by taking the average value of Cb and Cr as the human eyes is less sensitive to chrominance than Luminance. This can be accomplished as shown in figure 3.2

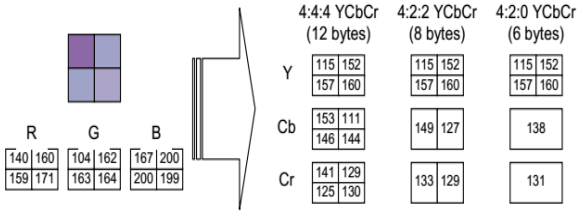


Fig 3.2 Conversion of RGB image into Y Cr Cb form

Once the image is in the proper color space, it is partitioned into 8X8 blocks. Each of the blocks is separately operated for JPEG compression.

3.3 Proposed Watermarking Technique

In this Research Paper, a watermarking based technique for image authentication is presented which makes use of the custom text watermark. The watermark is embedded in the Luminance Parameter of the image. Specifically, the watermark is embedded in the higher order DCT coefficients of the image so that it is preserved with lossy JPEG Compression.

Algorithm; Watermark Embedding in JPEG Image

Input: Raw Image;

Output: JPEG Compressed Watermarked Image.

1. Input the raw image (bitmapped) of any size.
2. Partition the image into Non-overlapping Blocks of Size 8X8 pixels
3. To each of the Block; do
   a. Transform the color values from RGB to Y, Cr, Cb as per the scheme. Each of the matrices Y, Cb, Cr have the dimensions 8X8.
   b. The Cr and Cb matrices are reduced to 4X4 based on averaging. This process is used in Lossy Jpeg compression and MPEG encoding of video. For mpeg video which operates on 16X16 blocks, it is called (4:2:2 encoding).
   c. The 8X8 Y block is transformed into frequency domain using DCT Transform. The result of this operation is that all high frequency components, which contain most of the information about the image, will get shift to the upper right corner of the matrix.

Genetic Approach:
Better PSNR
Robustness to Statistical Attacks

   d. The DCT block is quantized using Standard Quantization matrix used for JPEG Compression. The quantization matrix has low values at top left and significantly higher value at bottom right.
   e. A rounding-off operation is performed to make most of bottom left part of the matrix, having zeros. This step is the basis of JPEG Compression.
   f. Similar operation is applied to Cb and Cr blocks to implement image compression.
   g. The non-zero entries which remained in the top left of the DCT Transformed Y block are used for watermark embedding as explained in subsequent steps:
   h. Flip the LSB of the coefficients, starting from the one having second highest value, in accordance with the watermark bits. The steps I to J illustrates Genetic Algorithm approach to improve PSNR value.
   i. Select the coefficients whose absolute value are greater than or equal to 2^m. All such coefficients will be represented using at least m bits.
   j. Flip the 2nd LSB of all the coefficients pairs, taken two at a time and then re-compute Inverse DWT of the block to obtain RGB pixel block of size 8X8.
   k. Obtain the MSE between the original block and the Flipped Bit Block. Do this for subsequent coefficient pairs. If it is under permissible threshold, keep the change in the block, otherwise repeat the same process with next coefficient pairs.

The JPEG compressed file contains the DCT values of either 4:4:4 or 4:2:2 or 4:2:0 Chroma sampled blocks. Embedding the watermark into DCT values makes the scheme robust against JPEG compression. The Watermark detection and extraction algorithm is simple and fast on the same lines as the watermark embedding algorithm.

Algorithm; Watermark Detection in JPEG Image

1. Obtain the RGB Values from the raw image.
2. Partition the image into Non-overlapping Blocks of Size 8X8 pixels
3. To each of the Block; do
4. Transform the color values from RGB to Y, Cr, Cb as per the scheme. Each of the matrices Y, Cb, Cr have the dimensions 8X8, partition the image.
5. Obtain the Quantized DCT values of the Y block.
6. Extract the watermark from the LSB bits of the DCT coefficients.

3.4 Genetic Approach in Least Significant Bit (LSB) Encoding

The LSB encoding is, as the name indicates, in done in the bits of the coefficients of the DCT matrix obtained as a result of JPEG compression operation. In LSB encoding, the least significant bits of the coefficients are flipped in accordance with the message to be embedded. In this operation, 50 percent of the bits, who have values similar to the message to be encoded are flipped and remaining, approximately 50 percent bits remains as these were previously. This is illustrated in the simple schematic as shown in the figure 1.4.

Digital Data to be embedded

1	1	0	1	0	0	1

Original Data Array

67	89	65	58	72	81	92

Original Data Array (Binary)

10000 11	10110 01	10000 01	1110 10	10010 00	10100 01	10111 00

Data Array after LSB Encoding

10000 11	10110 01	10000 00	1110 11	10010 00	10100 00	10111 01

It is evident that after LSB encoding, 4 out of 7 entries are flipped. Thus, approximately 50 percent of the LSBs are flipped in LSB encoding. The data values, in decimal are shown in the subsequent row which indicates an interesting property of LSB transform and the way to include Genetic Approach for the minimization of the distortion done as a result of LSB encoding.

Original Data Array

67	89	65	58	72	81	92

Data Array after LSB Encoding

67	89	64	59	72	80	93

In the data array in which the watermarking bits are embedded through LSB Encoding, the only possibility that holds is as indicated below:

$$LSB\ Encoding\ in\ Real\ Numbers = \begin{cases} 1\ ; Number\ Remains\ Unchanged\ if\ the\ bit\ value\ matches\ the\ value\ of\ the\ LSB \\ 2 : If\ the\ number\ is\ Even, it\ gets\ converted\ into\ next\ higher\ Odd\ Value \\ 3 : If\ the\ number\ is\ odd, it\ gets\ converted\ into\ immediatly\ lower\ even\ value \end{cases}$$

The MSE of the data block can be computed as follows:

$$MSE = \frac{(67-67)^2 + (89-89)^2 + (64-65)^2 + (59-58)^2 + (72-72)^2 + (80-81)^2 + (93-92)^2}{7}$$

The MSE value comes out to be 0.5714

The Data Array after LSB Encoding is as shown:

10000 11	10110 01	10000 00	1110 11	10010 00	10100 00	10111 01

If the Second LSB is flipped in appropriate way, as shown, then the resulting encoded data array becomes:

10000 11	10110 01	10000 00	1110 11	10010 00	10100 00	10111 01

In this example, the 3rd , 4th and 6th values are changed in Second LSB positions. It results in an array shown as follows:

Data Array after Suitably Flipping Second Bit Position:

67	89	66	57	72	82	93

The MSE Value after flipping of second bit position is:

$$MSE = \frac{(67-67)^2 + (89-89)^2 + (66-65)^2 + (57-58)^2 + (72-72)^2 + (82-81)^2 + (93-92)^2}{7}$$

This value comes out to be exactly same as before; i.e. 0.5714, despite of the fact that now the statistical property of the image gets altered and now it can be made difficult of analyzed if the image consist of any data embedded in it with a view to implement covert communication.

In the proposed work, the first generation chromosomes are taken as coefficient pairs of original and watermarked image. From this pair, the second generation chromosomes are derived taking into consideration the PSNR values and the statistical properties of the blocks.

The flipping of the second LSB is required to be made under consideration of the following two objectives:

1. To keep the PSNR as high as possible.
2. To keep the statistical property of the image pixels as that of natural image so that it is difficult for the attacker to judge the presence of watermark in the image.

The operation of the flipping of Bit planes is illustrated in figure 3.3

To investigate the effect of LSB substitution, consider table 3.1:

TABLE 3.1

LSB SUBSTITUTION

Number	Binary Representation	Flipped LSB Value	Decimal	Flipped Second LSB	Decimal
101	1100101	1100100	100	1100111	103
102	1100110	1100111	103	1100100	100
103	1100111	1100110	102	1100101	101
104	1101000	1101001	105	1101010	106
105	1101001	1101000	104	1101011	107
106	1101010	1101011	107	1101000	104
107	1101011	1101010	106	1101001	105
108	1101100	1101101	109	1101110	110
109	1101101	1101100	108	1101111	111
110	1101110	1101111	111	1101100	108

It is evident that a change in 2nd LSB results in a change of magnitude of 2 in the original value. Likewise, change in third LSB results in a difference of 4 in the magnitude. It is clear that a substitution in higher order LSBs gives a more robust watermarking as compared to substitution in lower order LSBs. However, the more higher order LSBs are used, the more is the change in the values of the DCT coefficients and the higher is the Mean Square Error giving lower PSNR values. However, the image is more likely to be detected for the presence of watermark.

The Genetic Approach is illustrated by the following example:

ORIGINAL IMAGE

1100101	1100110	1100111
1101000	1101001	1101010
1101011	1101100	1101101

Original Zig-Zag Scan Value:

|101-102| + |102-104|+|104-107|+|107-105|+|105-103|+|103-106|+|106-108|+|108-109|

1+2+3+2+2+3+2+1 = 6+4+6= 16

WATERMARKED IMAGE

1100101	1100111	1100110
1101000	1101001	1101011
1101011	1101100	1101101

=

101	103	102
104	105	107
107	108	109

|101-103| + |103-104|+|104-107|+|107-105|+|105-102|+|102-107|+|107-108|+|108-109|

2+1+3+2+3+5+1+1 = 18

The Genetic Approach on the resultant LSB Flipped watermarked image works using selection of First and the next level pixel pairs, called chromosomes.

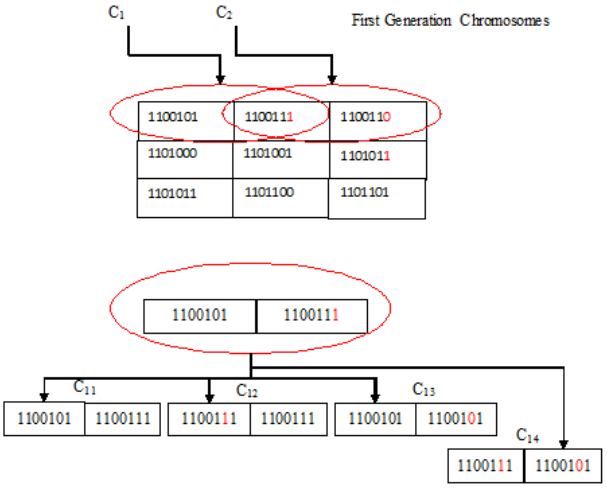


Figure 3.2 Reproductions of Second Generation Chromosomes from First Generation Chromosomes

In the above illustration, C_{11} is identical to C_1, as it represents the trivial case with no change. However, C_{12}, C_{13}, and C_{14} are different with second LSB's flipped as per the pixel pairs. The algorithm proceeds to find the optimal values of pixels to gives best possible PSNR, with the singularity of the block. The combination of pixel pairs for all the chromosome pair of 8x8 blocks are chosen to give the maximum PSNR value and yield optimum value of discrimination function.

The next generation chromosome is chosen on the basis of the value of the discrimination function so that the resultant block has lower discrimination function value as compared to the LSB flipped block.

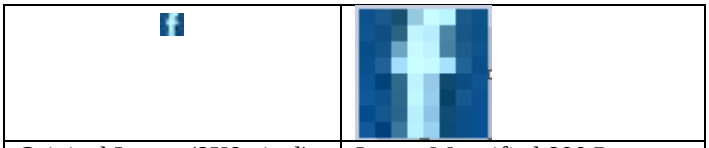
The value obtained above is called the discrimination function of the image block. If the new value of the discrimination function is greater than the previous value, then the block so obtained is called the Regular Block. Otherwise it is called a singular block. The example cited above is illustration, in which the pixel block after flipping turns out to be a Regular block. However, experimental results on a large number of natural images reveal that there is a significant increase in the number of Regular block after LSB embedding. The number of Regular blocs scan can be suitably controlled by suitably changing second LSB through genetic approach. This is illustrated in Section 4. Section 4 also illustrates the simulation steps for implementation of the proposed model.

.

IV ANALYSIS OF PROPOSED WORK

4.1 JPEG Image Watermarking

For the sake of illustration of the proposed scheme, an actual picture and a vivid picture of a sample image of 8X8 pixel is as shown:



Original Image (8X8 pixel)	Image Magnified 800 Percent

Figure 4.1 Sample FB logo of 8X8 Pixels for watermarking

The data values of the Red, Green and Blue Color planes of the Image are as follows:

RED:

13	26	25	149	200	186
16	15	43	192	183	74
7	19	108	199	189	70
10	32	165	201	197	165
13	0	47	190	148	15
17	15	45	193	151	6
5	21	43	185	142	17
18	0	61	186	154	13

GREEN:

81	89	80	201	252	245
84	78	98	244	238	133
77	85	165	251	243	129
80	98	221	255	251	224
84	67	106	244	202	73
88	82	103	247	206	66
76	88	101	238	196	76
89	65	119	241	208	75

BLUE:

142	140	111	222	255	255
145	129	129	*255	255	163
137	135	195	255	255	159
142	150	254	255	255	255
148	120	140	255	230	110
152	137	140	255	236	103
142	143	139	255	230	118
155	123	157	255	242	116

The image consists of a total of 64 pixels and each pixel requires 24 bits (8 each for Red, Green and Blue) color information. Thus, the number of bits required to store this 8X8 pixel image is:

8X8X(8+8+8) = 1536 bits or 1.5 kb

However the size of the jpg files, on windows OS is 694 bits. Thus a significant compression can be achieved using JPEG algorithm.

The conversion of the RGB color values of YCrCb color space can be done using the equations as mentioned in Section 1. Using those relations, the corresponding Y, Cb and Cr matrices are as shown:

Luminance (Y)

74	81	74	177	219	212
77	72	89	213	208	118
70	77	146	219	212	115
73	88	195	221	218	196
76	62	95	213	178	67
80	75	93	215	182	61
70	80	92	208	174	70
81	61	107	210	184	69

Chrominance (Cr)

94	97	102	104	105	101
94	97	102	104	103	100
93	95	101	105	103	100
93	95	101	104	104	100
92	95	100	103	102	100
92	95	100	104	102	99
92	95	100	104	102	99
92	95	100	103	102	98

Chrominance (Cb)

165	160	150	145	137	141
165	160	150	141	144	150
165	160	150	137	141	150
166	161	151	136	138	150
167	161	152	141	148	153
167	162	153	140	149	153
168	162	153	143	151	155
168	163	153	142	151	155

Let the four color segments of Cr be Cr(1,1), Cr(1,2), Cr(2,1) and Cr(2,2) with notation have its usual meaning.

The difference matrix can be computed as follows:

Cr(1,1) - Cr(1,2)

-11	-4	5	10
-9	-3	6	10
-10	-5	5	11
-11	-5	6	11

Similarly

Cr(2,1) - Cr(2,2)

-10	-5	4	10
-10	-4	5	11
-10	-4	5	12
-10	-3	5	11

Thus, it is evident that enough redundant information is available in RGB color space that can be eliminated to achieve substantial compression.

In standard JPEG compression 4:2:2 sampling is used. This means that the blocks used for DCT compression are

Y(1,1)	Y(1,2)	Avg. {Cr(1,1), Cr(1,2)}	Avg. {Cb(1,1), Cb(1,2)}
Y(2,1)	Y(2,2)	Avg. {Cr(2,1), Cr(2,2)}	Avg. {Cb(2,1), Cb(2,2)}

The DCT of the Y color channel is as follows:

DCT (Y)

933.125	-1.0354	375.147	-4.61446	177.875	20.3444	-44.9868	-16.7534
60.6392	-37.843	-36.8311	68.6022	-41.5439	-34.445	41.6456	-18.7496
-28.8857	-20.361	19.7433	43.1954	13.7209	-17.7556	-14.3362	-17.9424
-37.5465	-14.985	30.7531	30.3105	16.6432	-8.95986	-26.6884	-23.8698
26.375	-14.597	-13.7697	29.2688	-27.375	-10.7525	41.5578	-8.05123
48.5242	-9.3793	-23.0585	19.7282	-51.9214	-20.0189	37.1038	-9.10254
5.06458	-0.5173	-0.33623	0.07516	0.13447	0.16627	0.24067	10.05937
-38.3631	-0.0614	18.5070	-10.9376	23.0047	0.35132	-20.6853	0.051581

The Standard Quantization matrix in JPEG 2000 is shown in table

Q =

16	18	19	19	24	40	5
12	12	12	19	26	58	6
14	16	16	24	40	57	6
14	17	22	29	51	87	8
18	22	37	56	68	109	1
24	35	55	64	81	104	1
49	64	78	87	103	121	1
72	82	95	98	112	100	1

The pairwise division operation of the DCT matrix with Quantization matrix gives

DCT/Q =

58.32031	-0.09414	-37.5147	-0.2884	7.411458	0.508611	-0.88209	-0.27465
5.053274	-3.1536	-2.60979	3.610643	-1.59784	-0.59388	0.694094	-0.3409
-2.06326	-1.56629	1.219333	1.799808	0.343023	-0.3115	-0.20777	-0.3204
-2.68189	-0.88148	1.397871	1.045198	0.326338	-0.10299	-0.33361	-0.385
1.465278	-0.66352	-0.37215	0.522659	-0.40257	-0.09865	0.403474	-0.10456
2.021842	-0.26798	-0.41924	0.308253	-0.641	-0.19249	0.328352	-0.09894
0.103359	-0.00808	-0.00431	0.000864	0.001306	0.001374	0.002006	0.099598
-0.53282	-0.00075	0.194811	-0.11161	0.2054	0.003513	-0.20083	0.000521

The rounding operation gives:

Round(DCT/Q) =

58	0	-38	0	7	1
5	-3	-3	4	-2	-1
-2	-2	1	2	0	0
-3	-1	1	1	0	0
1	-1	0	1	0	0
2	0	0	0	-1	0
0	0	0	0	0	0
-1	0	0	0	0	0

In this rounded matrix, a large number of elements are zero. Only the nonzero values are required to be saved. The matrix is scanned in zig-zag way and the elements which are required to be saved are:

58	5	0	-38	-3	-2	-3	-2	-3	0	7	1	-2	2	1	-1	2

The LSB encoding will be made in these bit planes for the purpose of watermark embedding. The watermarking is performed in LSB plane of the quantized values of the DCT coefficients.

4.2 Watermarking Simulation Results

For the sake of illustration, the given image of lena (512X512) is partitioned into 64X64 blocks, giving a total of 64 blocks.

Figure 4.2 Original Image of Lena, Dimension 512X512

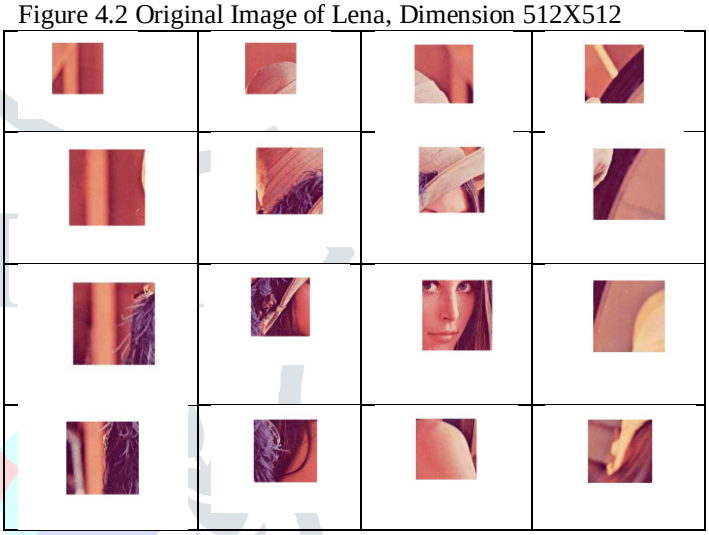


Fig 4.3 Partitions of the Original Image, dimensions 64X64 each

In practice, each of the 8X8 block is separately processed for the purpose of watermark embedding. Considering block #11, for the processing of the operation of watermarking, the watermarked image can be obtained following the steps as outlined in Section 3.

4.3 Performance Evaluation

The mean square error for the above specified technique for the FB.jpg file can be computed by pair wise differencing the original image with the watermarked image. The square of this difference is successively added and then divided by the total number of pixels (in this case, 8 X 8). This gives the mean of the square of the error. For the image under consideration, the MSE comes out to be 172.41.

The PSNR value of corresponding to this value of MSE is 7.277039

The PSNR values corresponding to some benchmark images (shown in Figure 4.2) is shown in table.

Barbara

Cameraman

Baboon

Figure 4.4 Benchmark Images for Performance Evaluation

The MSE and PSNR values for the benchmark images and the comparison with Oh Jin Kwon et. al. [1] are shown in table 4.1.

TABLE 4.10
MSE AND PSNR VALUES OF THE BENCHMARK IMAGES

	Proposed		Oh Jin Kwon et. al. [1]	
Image	MSE	PSNR	MSE	PSNR
Barbara	11712.3	7.44437	11730.3	7.43770501
Camraman	12557.1	7.1419	12594.1	7.12912534
Baboon	12209.7	7.26376	12245.7	7.25097809

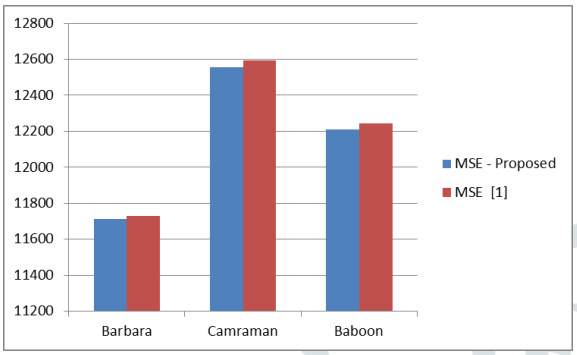


Figure 4.5 Comparison of MSE Values of Images with those of Oh Jin Kwon et al. [1]

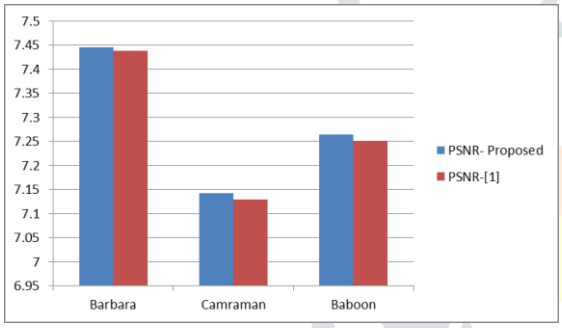


Figure 4.6 Comparison of PSNR Values of Images with those of Oh Jin Kwon et al. [1]

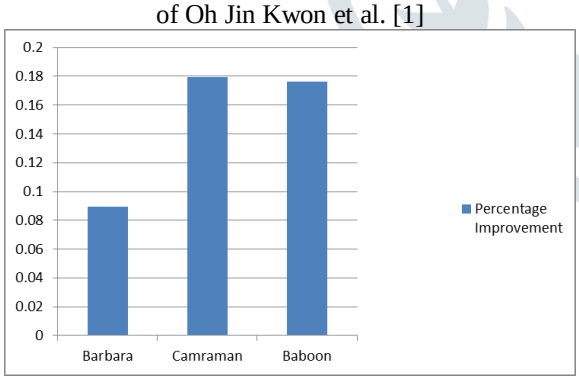


Figure 4.7 Percentage Improvement in PSNR Values

The Genetic Approach flips the second LBS to make the watermarking scheme resistant against RS steganalysis attack. After the flipping of second LSB values, the performance matrix is as shown:

TABLE 4.11
MSE AND PSNR VALUES OF THE BENCHMARK IMAGES, AFTER FLIPPING OF SECOND LSB

	MSE - Proposed	PSNR-Proposed	MSE [1]	PSNR-[1]
Barbara	11719.32	7.441779479	11730.32	7.437705
Camraman	12571.12	7.137063888	12594.12	7.129125
Baboon	12221.67	7.259498078	12245.67	7.250978

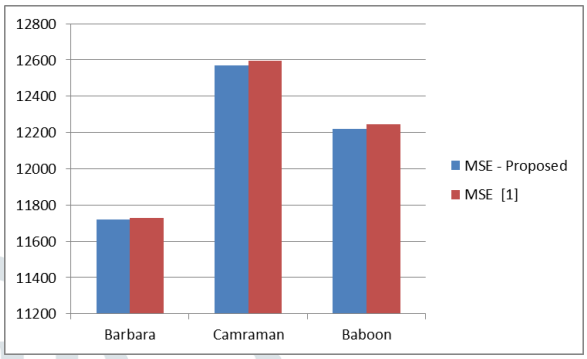


Fig. 4.8 Comparison of MSE Values, After Genetic Algorithm Application, of Images with those of Oh Jin Kwon et al. [1]

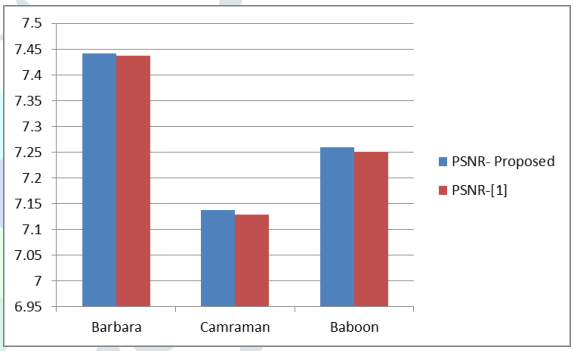


Figure 4.9 Comparisons of PSNR Values, After Genetic Algorithm Application, of Images with those of Oh Jin Kwon et al. [1]

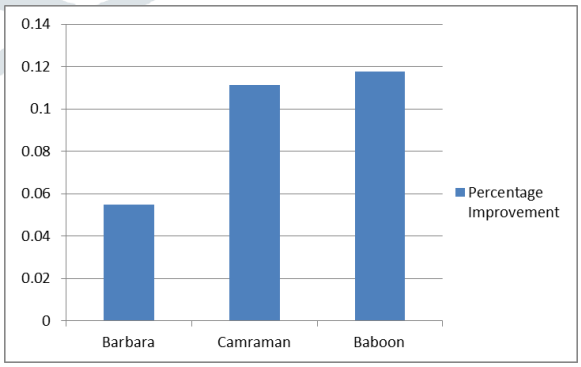


Figure 4.10 Percentage Improvement in PSNR Values, After Genetic Algorithm Application

Above results establishes that Genetic Algorithm based watermarking can be successfully applied in digital watermarking, with acceptable PSNR, to implement a robust watermarking scheme. Section 5 analyses the results and concludes the Research Paper.

.

V CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

A blind JPEG compression based watermarking algorithm, using LSB encoding in DCT coefficients, is proposed in this Research Paper. In this scheme, the statistical properties of the pixels are also altered thereby making it difficult to detect the presence of watermark through steganalysis. The watermarking embedding is applied to non-overlapping blocks of the image, thereby making it robust against cutting and cropping attacks. The simulation results prove that the proposed technique has good PSNR and MSE as compared to the benchmark techniques.

6.2 Future Scope

As the future scope of this work, a RST invariant watermarking approach is to be formulated which is resistant to attacks like print and scan attacks. Moreover, the watermarking techniques needs to be semi fragile in accordance with the need of time, so that it can provide tempering protection and at the same time, embed the watermark so robustly that no attacker can destroy or remove the watermark. As a future aspect, of this work, the watermark is to embedded in the matrices much more evenly so as to provide better perceptual quality of the watermarked image.

REFERENCES

[1] Kwon, Oh-Jin, Seungcheol Choi, and Beomyeol Lee. "A Watermark-Based Scheme for Authenticating JPEG Image Integrity." IEEE Access 6 (2018): 46194-46205.

[2] Schelkens, Peter, et al. "The JPEG 2000 family of standards." Wavelet Applications in Industrial Processing Vi. Vol. 7248. International Society for Optics and Photonics, 2009.

[3] Ibraheem, Noor A., et al. "Understanding color models: a review." ARPN Journal of science and technology 2.3 (2012): 265-275.

[4] Birney, Keith A., and Thomas R. Fischer. "On the modeling of DCT and subband image data for compression." IEEE transactions on Image Processing 4.2 (1995): 186-193.

[5] Tao, Hai, et al. "Robust image watermarking theories and techniques: A review." Journal of applied research and technology 12.1 (2014): 122-138.

[6] Wang, Ran-Zan, Chi-Fang Lin, and Ja-Chen Lin. "Image hiding by optimal LSB substitution and genetic algorithm." Pattern recognition 34.3 (2001): 671-683.

[7] Petitcolas, Fabien AP. "Watermarking schemes evaluation." IEEE signal processing magazine 17.5 (2000): 58-64.

[8] Cimato, Stelvio, and Ching-Nung Yang, eds. Visual cryptography and secret image sharing. CRC press, 2017.

[9] Shih, Frank Y. Digital watermarking and steganography: fundamentals and techniques. CRC press, 2017.

[10] Cheung, W. N. "Digital image watermarking in spatial and transform domains." 2000 TENCON Proceedings. Intelligent Systems and Technologies for the New Millennium (Cat. No. 00CH37119). Vol. 3. IEEE, 2000.

[11] Hernández, Juan R., and Fernando Pérez-González. "Statistical analysis of watermarking schemes for copyright protection of images." Proceedings of the IEEE 87.7 (1999): 1142-1166.

[12] Sreenivas, K., and V. Kamkshi Prasad. "Fragile watermarking schemes for image authentication: a survey." International Journal of Machine Learning and Cybernetics 9.7 (2018): 1193-1218.

[13] Qi, Xiaojun, and Xing Xin. "A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization." Journal of Visual Communication and Image Representation 30 (2015): 312-327.

[14] Deshmukh, Sneha A., and P. B. Sambhare. "An Authentication of Secretely Encrypted Message Using Half-Tone Pixel Swapping From Carrier Stego Image." IJCSIT) International Journal of Computer Science and Information Technologies6.3 (2015): 2409-2015.

[15] Su, Qingtang, and Beijing Chen. "Robust color image watermarking technique in the spatial domain." Soft Computing 22.1 (2018): 91-106.

[16] Luo, Xiang-Yang, et al. "A review on blind detection for image steganography." Signal processing 88.9 (2008): 2138-2157.

[17] Kim, Changick. "Content-based image copy detection." Signal Processing: Image Communication 18.3 (2003): 169-184.

[18] Chanu, Yambem Jina, Themrichon Tuithung, and Kh Manglem Singh. "A short survey on image steganography and steganalysis techniques." 2012 3rd National Conference on Emerging Trends and Applications in Computer Science. IEEE, 2012.

[19] Singh, Prabhishek, and R. S. Chadha. "A survey of digital watermarking techniques, applications and attacks." International Journal of Engineering and Innovative Technology (IJEIT) 2.9 (2013): 165-175.

[20] Huang, Fangjun, et al. "Reversible data hiding in JPEG images." IEEE Transactions on Circuits and Systems for Video Technology 26.9 (2015): 1610-1621.

[21] Susanto, Ajib, Eko Hari Rachmawanto, and Christy Atika Sari. "A robust non-blind image watermarking method using 2-level HWT-DCT." 2018 International Seminar on Application for Technology of Information and Communication. IEEE, 2018.