DOI: 10.21917/ijivp.2010.0017

A ROBUST DIGITAL IMAGE WATERMARKING ALGORITHM USING DNA SEQUENCES

V. Santhi[1] and Arunkumar Thangavelu
[1]*School of Computing Sciences and Engineering, VIT University, Tamil Nadu, India*
E-mail: vsanthi@vit.ac.in[1]

Abstract
Digital watermarking technique emerged as a tool for protecting the multimedia data from copyright infringement. In digital watermarking an imperceptible signal is embedded into the host image, which uniquely identifies the ownership. In the proposed algorithms, DNA sequence is used as a digital watermark, as the DNA sequences are unique and difficult to copy. This paper proposes two algorithms namely content based watermark algorithm using DNA sequence (CBDNA) and user specified watermark algorithm using DNA sequence (USDNA). In CBDNA the DNA sequence is generated from the cover data itself whereas in USDNA input data is chosen by the user and DNA sequence is generated based on the input data. These DNA sequences serve as a watermark for the cover data. The quality of the cover image and extracted watermark is measured using peak signal to noise ratio (PSNR) and normalized correlation (NC) respectively. The calculated values are tabulated and it shows that the proposed algorithm is withstanding many attacks, since watermark is available in all the frequency range of cover data.

Keywords:
Deoxyribonucleic Acid (DNA), Discrete Wavelet Transform (DWT), Content based watermarking algorithm using DNA sequence (CBDNA), User specified watermarking DNA sequence (USDNA)

1. INTRODUCTION

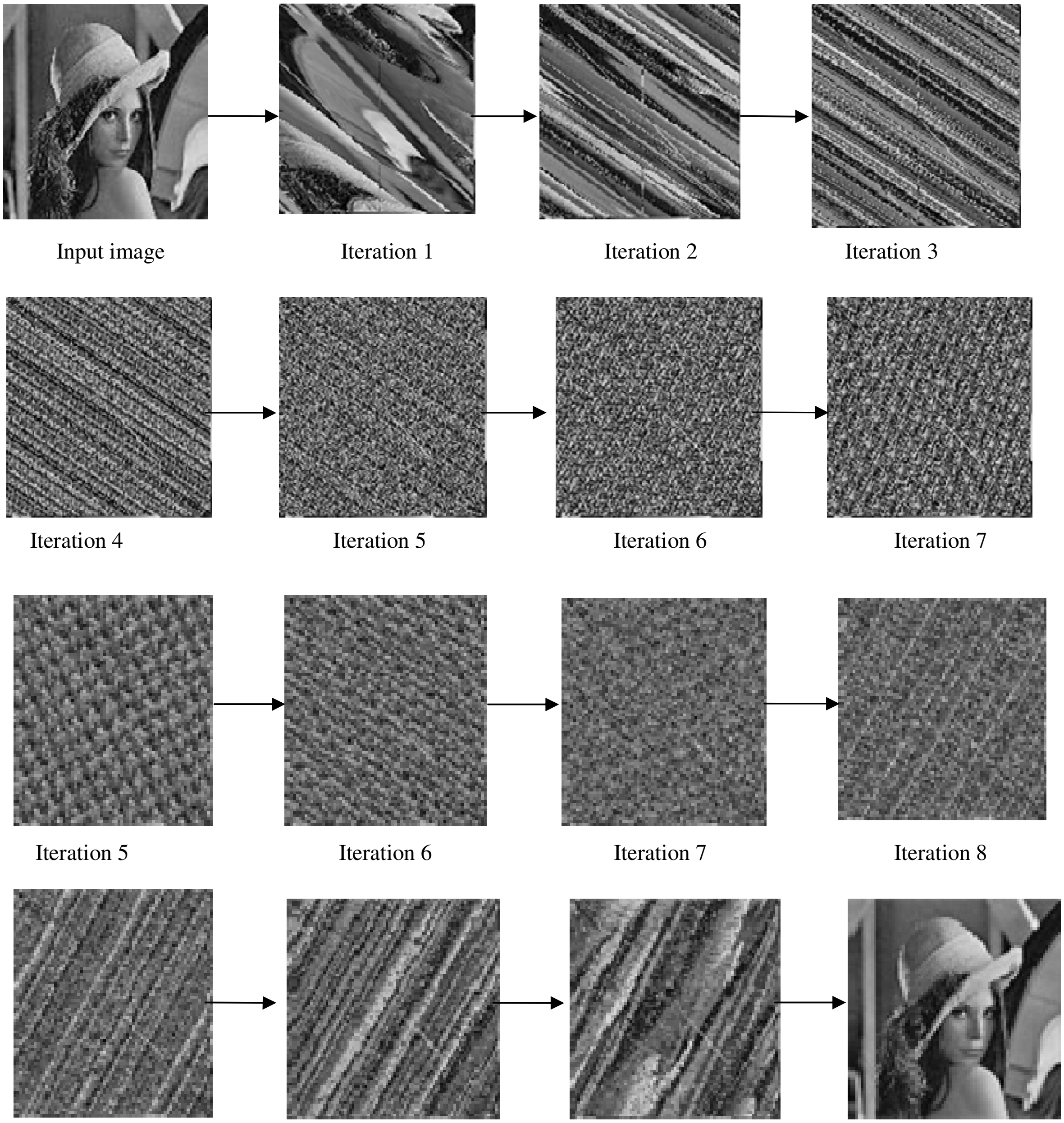
In recent years the phenomenal growth of the Internet has highlighted the need for mechanisms to protect ownership of digital media. Exactly identical copies of digital information, images, text or audio, can be produced and distributed easily. In such a scenario, we need to differentiate between the artist and the plagiarist [1]. Digital watermarking is a technique that provides a solution to the longstanding problems related to copyrights of digital data. In order to protect multimedia data many techniques are available including cryptography, steganography, digital watermarking and information hiding. Among these techniques digital watermarking is gaining popularity in the present days to protect copyright of multimedia data. The applications of digital watermarking include active ownership verification, copyright protection, finger printing and image authentication.

Digital watermarking is defined as a process of hiding a piece of secret information (watermark) in cover data which can be extracted later for ownership verification, Copyright protection and for image authentication [7]. A digital watermark can be any piece of information about users such as date of birth, user name, telephone numbers and any user selected input data. Digital watermarking can be classified according to the domain in which watermark is embedded. In spatial-domain, the watermarking is done by changing the intensity value of pixels [3]. This kind of watermarking is simple and computation complexity is very low, since no frequency transform is needed. In frequency-domain watermarking, it embeds the watermark by changing the frequency components. Many transformation techniques are available to transform images from time domain to frequency domain including discrete Fourier transformation (DFT), discrete cosine transformation (DCT) [5][9], discrete wavelet transformation (DWT) [10] and discrete Hadamard transformation (DHT). Frequency domain transformation approach is more complex when compared to spatial domain transformation but has the advantage of robustness to image processing operations which may be unintentional and intentional.

According to how the watermark is being detected and extracted, digital watermarking can be classified into blind watermarking technique and non-blind watermarking technique. In blind watermarking, the watermark detection and extraction does not depend on the availability of original image [2]. The drawback is when the watermarked image is seriously destroyed; watermark detection will become very difficult. In non-blind watermarking, the watermark can be detected if only the original image is available [15].

In [10], DNA sequences are being used in the field of information hiding, where the input text message is encoded into a DNA sequence. This text message is embedded into a host DNA using substitution cipher method. The output obtained is an encoded DNA sequence with the input message embedded into it.

In this paper two new algorithms have been proposed for hiding a unique DNA sequence in a cover data. This proposed technique could be used to identify the owner of the cover data in a unique way and similarly it could also be used for authentication and copyright protection. Proposed algorithms could be classified as non-blind watermarking algorithm since it requires original cover data to extract the watermark. The discrete wavelet transformation technique is used to transform an image from time domain to frequency domain. In first algorithm named CBDNA the watermark is generated based on the content of the cover image whereas in second algorithm named USDNA the user specified input is considered for generating unique DNA sequence which is used as watermark.



Input image

Iteration 1

Iteration 2

Iteration 3

Iteration 4

Iteration 5

Iteration 6

Iteration 7

Iteration 5

Iteration 6

Iteration 7

Iteration 8

Fig. 1 Output of Arnold Transformation in various iterations

In section II basics of DNA and its usage in computing is given and section III elaborates an Arnold cat map transformation. Section IV highlights the review of related works on DNA computing field and in section V, the proposed algorithms are explained. Section VI discusses the performance of our proposed algorithms. Section VII concludes our work with the result obtained.

2. DNA IN COMPUTING

2.1 REVIEW STAGE

DNA is called as the ‘blue print of life’, because it contains the whole information about a particular organism. DNA over millions of years, have demonstrated their effectiveness as a coding medium for the instruction set that governs and propagates living things. DNA sequences, themselves, cannot be patented, and rightly so. However, the nature of DNA is such that, once the real work of isolating and identifying a useful sequence has been done, copying is trivial [8]. DNA contains a sequence of 4 nucleotides which are binded together to form a long nucleotide chain. The nucleotides are Adenine (A), Guanine (G), Cytosine(C) and Thymine (T) [14][11].

DNA is a coding medium that encodes all the genetic information of the human body. However to represent a DNA sequence for computational purpose, we have to code the DNA into binary bits. If this can be done, the DNA sequences can be used for computational purposes. The nucleotides present in the

DNA sequence is used to encode binary information. A proper understanding of the encoded binary bits of the DNA sequence would facilitate to use the DNA for computation [12].

3. ARNOLD CAT MAP TRANSFORMATION

To encrypt images in the proposed algorithms Arnold cat map transformation technique is used [16]. In this transformation the pixel coordinates of the images undergo transformation based on a transformation function. The resultant pixel values are scrambled and produce encrypted images. The transformation function used for encrypting images is given in Eq. (1). Fig 1 shows that the Arnold cat map encrypts the image in each iteration, as this is periodic in nature and after certain iteration the pixels get back to its original position and thus image is decrypted.

$$T\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}x+y\\x+2y\end{bmatrix} \bmod n \qquad (1)$$

4. REVIEW OF RELATED WORK

Leonard Adleman [17] published the first paper on the use of DNA to solve Hamiltonian path problem in 1994. In this work DNA molecules are synthesized represent the edges in a Hamiltonian path problem. Later after performing certain reactions, a new set of DNA sequences are produced as answer. It is said that he took one second to come up with the answer but it took him one week to dig out the answer from the DNA soup.

Mohd Saufee Muhammad et al. [6] have solved the elevator scheduling problem which consists of 2 elevators and 6 floors. Using the weighted graphs, DNA sequences are initially synthesized and a set of reactions are performed on these sequences. The reactions are results in the resultant solution.

In [13], S. A. Tsaftaris, et al have proposed a procedure for storing and retrieving digital signals based on DNA sequences. In which the digital signals are encoded into DNA sequences by using DNA codeword design. The digital signals are designed based on the constraints including the noise tolerant constraint (NTC). To design a DNA based database, we consider both invitro (within the test tube) for short term storage and in vivo (within a living organism) for long term storage. The short term storage of digital signals is done inside a test tube whereas the long term storage of digital signals is done by storing it inside humans.

In paper [4] one-time-pad mechanism based on DNA sequences is designed for encryption. There are two methods proposed; the first method translates the fixed length DNA plain code sequence to DNA cryptograph sequence according to the defined mapping graph whereas the second is called exclusive-or method, which uses biological techniques to carry out exclusive-or operation of DNA plain code and cipher key sequence. These two methods provide a high level of security.

5. PROPOSED SYSTEM

The main objective of the proposed systems is to design a new watermarking algorithm using DNA concepts. In this paper two algorithms have been proposed and it is named as CBDNA and USDNA. In CBDNA a unique DNA sequence is generated based on the host image and used as watermark which is embedded into the host data. In USDNA the user input is used to generate a DNA sequence and this is used as a watermark which is hidden into the host data. The DNA sequence generated remains unique to the user and also unique to the input data.

In CBDNA input image is divided into many numbers of smaller blocks. The user is allowed to choose any one particular block from the available blocks. The block chosen remains as a key to the user. The selected block is encrypted using Arnold cat map algorithm, a DNA sequence is generated from the encrypted block. The algorithm embeds the watermark in the frequency domain of the cover image. A transformation technique called, discrete wavelet transform (DWT) is applied to the cover image. This converts the cover image into different wavelets corresponding to low, medium and high bands of frequencies. The watermark is hidden into the low frequency band of the cover image after multiplying it with a scalar factor. An inverse DWT of the image gives the watermarked image.

In USDNA, the user input is considered as a piece of data to be hidden which is encrypted using Arnold cat map and a DNA sequence is generated based on the encrypted data. The cover image is transformed using discrete wavelet transformation technique and watermark is hidden into the wavelet coefficients of cover data after multiplying it with a scalar factor.

5.1 CONTENT BASED WATERMARKING ALGORITHM USING DNA SEQUENCE – CBDNA

In this algorithm the input image or cover image is converted into many blocks of size m x m and any one of the block is selected as a primer block using a key. The primer block is used to generate DNA sequence after encryption. The architecture of embedding and extraction process of CBDNA is given in Fig.2. The cameraman image of size 512 X 512 is considered as test image.

5.1.1. Embedding Algorithm

The steps for embedding the watermark in CBDNA are as follows:

1. Let A be the input image which is divided into many number of smaller blocks of size N x N and a particular block called primer block is selected by the user.

   $[a_1,a_2,a_3,a_4,\ldots a_n] = \text{Blocking}(A) \qquad (2)$

2. Let A be the input image which is divided into many number of smaller blocks of size N x N and a particular block called primer block is selected by the user.

   $[a_1,a_2,a_3,a_4,\ldots a_n] = \text{Blocking}(A) \qquad (3)$

3. The primer block, say a_1 of size S x S is encrypted using Arnold Transformation.

```
for x=1 to s
    for y = 1 to s
        $T\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}x+y\\x+2y\end{bmatrix} \bmod n$        (4)
    end
end
```

   where *x* and *y* represents the co-ordinates of the pixel values of block a_1.

4. Each pixel in the encrypted block is converted into sequence of binary bits. Two binary bits are combined and encoded as a single nucleotide as below

   A = 00, G =01, C=10, T=11
5. A look up table is created in which there is an entry for all the unique DNA sequences and a unique random number is assigned for each sequences.
6. After encrypting and converting the primer block into DNA sequence, the random integer number is assigned for each DNA sequence based on the look up table to create a unique watermark.
7. The input image is transformed using discrete wavelet transformation technique to decompose it into four frequency bands.

   [cA1, cH1, cV1, cD1] = dwt2 ('A' , 'dB1') (5)
8. The watermark can be hidden in any one of the quadrants of the cover image.

   $cA_{ij}= cA1_{ij}+\alpha*w_{ij}$ (6)

   where cA1 is the low frequency band of the cover image, w is the watermark matrix and α is the scaling factor used.
9. Apply inverse wavelet transformation technique to get the watermarked image.

   WI=idwt2(cA,cH1,cV1,cD1) (7)

5.1.2. Extraction Algorithm

The steps for embedding the watermark in CBDNA are as follows:

1. The watermarked image and the cover image are taken as an input for extraction. Let WI represent the watermarked image and A represent the original image
2. The images are transformed into frequency domain by DWT. The respective quadrant where the watermark has been hidden is selected.

   [cA2, cH2, cV2, cD2]=dwt2 ('WI' , 'db1') (8)

   [cA3, cH3, cV3, cD3]=dwt2 ('A' , 'db1') (9)
3. The watermark is extracted by subtracting the corresponding pixel values from the original image and then dividing the output with a scaling factor.

   $cA_{ij} = cA2_{ij} – cA3_{ij}$ (10)

   where cA2 is the frequency coefficients of the watermarked image and cA3 is the frequency coefficients of the original image.
4. The watermark matrix generated, is converted in to a DNA sequence using look-up table, where each number is mapped to its corresponding nucleotide sequences.
5. Based on the DNA code word table, the DNA sequences are converted into integers. 00=A,01=G,10=C,11=T
6. These integers now represent the encrypted image block. The decryption is performed by applying the Arnold transformation technique.

   $$T\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}x+y\\x+2y\end{bmatrix} \bmod n \qquad (11)$$
7. The NC values are calculated for the extracted watermark and the original watermark. This determines the amount of similarity exists in both blocks.

5.2. USER DATA BASED WATERMARKING ALGORITHM USING DNA SEQUENCE – USDNA

In this scheme, the watermark is generated based on the user selected input. So the proposed algorithm named as USDNA. The user selected input is encrypted and used to generate DNA sequence using AGCT nucleotides. The encrypted DNA sequence is embedded into the cover image in transform domain. Discrete wavelet transformation technique is used to bring the transform domain of the cover image. The DNA sequences thus generated remains unique to the input data. The generated unique DNA sequences for the input data provide a step of authentication for the user. The architecture diagram for embedding and extracting the watermark is given in Fig.3. The cameraman image of size 512 X 512 is considered as test image.

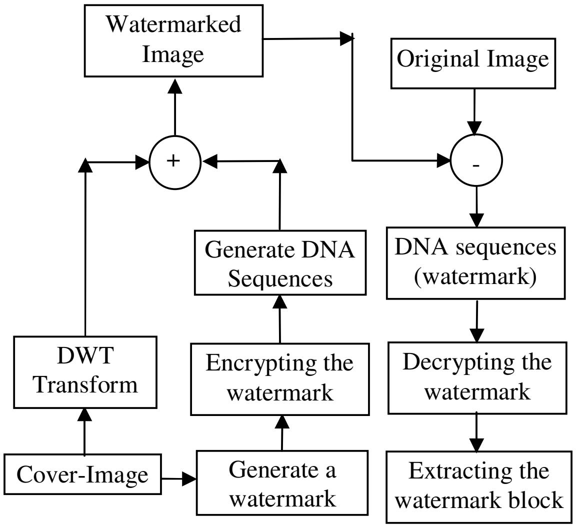


Fig. 2 Architecture diagram for CBDNA

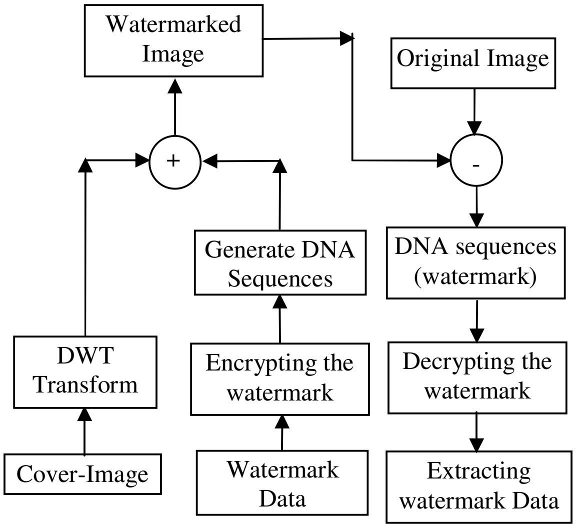


Fig. 3 Architecture diagram for USDNA

5.2.1. Embedding Algorithm

The steps for embedding the watermark in USDNA are given below:

Let A1 and A be the watermark image and the input image chosen by the user which is of size N x N and M x M respectively.

1. The watermark image A1 of size N x N is encrypted using Arnold Transformation.

```
for x=1 to N
    for y = 1 to N
        $T\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}x+y\\x+2y\end{bmatrix} \bmod n$          (12)
    end
end
```

   where x and y represents the co-ordinates of the pixel values for $A1_1$.

2. Each pixel in the encrypted block is converted into sequence of binary bits. Two binary bits are encoded by a single nucleotide as given below.

   A = 00, G =01, C=10, T=11

3. A look up table is created in which there is an entry for all the unique DNA sequences and a unique random number is assigned for each sequences.
4. After encrypting and converting the input data into DNA sequence, the random integer number is assigned for each DNA sequence based on the look up table to create a unique watermark.
5. The input image or cover image is transformed using discrete wavelet transformation technique to decompose it into four frequency bands.

   $$[cA1, cH1, cV1, cD1] = dwt2(\text{'A'}, \text{'dB1'}) \quad (13)$$

6. The watermark is hidden in one of the quadrants of the cover image. The resultant gives the watermarked image.

   $$cA=cA1_{ij}+\alpha*w_{ij} \quad (14)$$

   where cA1 is the low frequency component of the cover image, w is the watermark matrix and α is the scaling factor.

7. An inverse transformation gives the resultant watermarked image.

   $$WI=idwt2(cA,cH1,cV1,cD1) \quad (15)$$

5.2.2. Extraction Algorithm

The steps for extracting the watermark for USDNA are described as follows:

1. Let WI represent the watermarked image and A represent the cover image respectively.
2. The watermarked image and the original image are converted into frequency domain by DWT. The respective quadrant where the watermark has been hidden is selected.

   $$[cA1,cH1,cV1,cD1]=dwt2(WI','db1') \quad (16)$$

   $$[cA2,cH2,cV2,cD2]=dwt2(A','db1') \quad (17)$$

3. The watermark is extracted by simply subtracting the pixel values from the original image and then dividing the output with a scaling factor.

   $$cA_{ij}=cA1_{ij}-cA2_{ij} \quad (18)$$

   where cA1 is the low frequency coefficients of the watermarked image and cA2 is the low frequency coefficients of the original image.

4. The watermark matrix generated, is converted to a DNA sequence from the Look-up table, where each number is mapped to its corresponding nucleotide sequences.
5. These nucleotide sequences are now to be converted into the pixel values of the image block. Based on the DNA code word table, the DNA sequences are converted into integers , 00=A, 01=G, 10=C, 11=T
6. These integers now represent the encrypted image. The decryption algorithm is performed. This is again done by applying the same transformation function on the receiver side. The image watermark is then generated.

   $$T\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}x+y\\x+2y\end{bmatrix} \bmod n \quad (19)$$

   The pixel values after a particular number of iterations retain the original coordinate position.

7. The NC values are calculated for the extracted watermark and the original watermark. This determines the amount of similarity exists in both blocks.

6. PERFORMANCE ANALYSIS

The performance of the proposed algorithms is measured by embedding watermark in all the frequency bands of the cover image. The quality of the watermarked image is then measured using peak signal to noise ratio (PSNR). PSNR is the objective quality which measures the quality of the watermarked image. The quality of the extracted watermark is measured in terms of their similarity. The equations for calculating the PSNR and the NC values are given in (19) and (20) respectively.

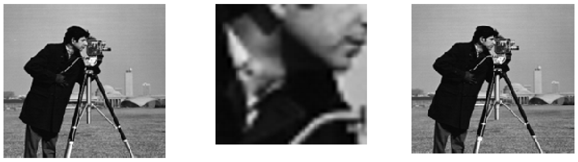
$$MSE=\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(f(i,j)-f'(i,j))^2 \quad (20)$$

$$PSNR=10\log\log_{10}\left[\frac{255^2}{MSE}\right] \quad (21)$$

where *f(i ,j)* and *f'(i,j)* represent the pixel values of the original host image and the watermarked image. The parameters *m* and *n* specifies the row and column of the original and the watermarked image. The similarity between the original watermark and the extracted watermark is given in (21)

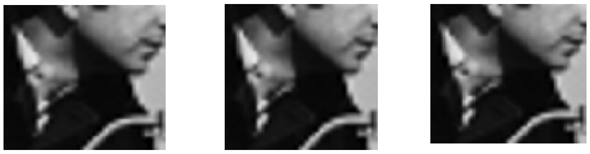
$$NC=\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}w(i,j)*w_e(i,j)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m}w^2(i,j)}\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m}w_{e\,(i,j)}^2}} \quad (22)$$

where w and we represents the original and the extracted watermark respectively.



(a) Original Image (b) Watermark block (c) Watermarked mage

Fig. 4



(a) Low Frequency (b) Middle Frequency (c) High Frequency

Fig. 5 Extracted watermarks before the attacks

6.1 PERFORMANCE ANALYSIS OF CBDNA

The cover image, watermark and the watermarked image are shown in Fig. 4. It is clear from the results that the algorithm is imperceptible and the calculated PSNR shows that the watermarked image is of good quality when hidden in the low frequency part of an image than middle and high frequency components. The extracted watermark from the three frequency levels under normal conditions without any attacks is shown in Fig. 5. The peak to signal ratio (PSNR) and the similarity measure (NC) of the extracted watermark is tabulated in Table 1.

The robustness of the algorithm is tested against various attacks such as cropping, Gaussian noise, salt and pepper noise, histogram equalization and rotation. The PSNR value of the extracted watermark from the low, middle and the high frequency bands are shown in Table 2. The robustness of the algorithm is tested against various attacks such as cropping, Gaussian noise, salt and pepper noise, histogram equalization and rotation. The proposed algorithm CBDNA resists attacks such as salt and pepper noise, Gaussian noise, cropping and histogram equalization, when watermark is hidden in low frequency components rather than middle and high frequency components but not robust to rotation attack in low frequency. This algorithm is robust to rotation attack when information is hidden in the high frequency components.

Table.1. PSNR values of the original and the watermarked image under normal conditions

Quality Measured	Low Frequency	Middle Frequency	High Frequency
PSNR	34.581	33.102	32.9448
NC	0.9805	0.99	0.9965

Table.2. calculated PSNR values after various attacks when watermark is hidden in low, middle and high frequency bands

Attacks	L-F PSNR	M-F PSNR	H-F PSNR
Salt & Pepper attack (Mean = 0.2)	32.2183	28.5371	27.4435
Gaussian Noise (Mean=0.01, Variance=0.5)	34.2257	32.552	31.3521
Rotation (90 degrees)	37.914	35.12	43.314
Cropping	35.5295	31.521	28.3256
Histogram Equalization	32.12	30.145	31.045

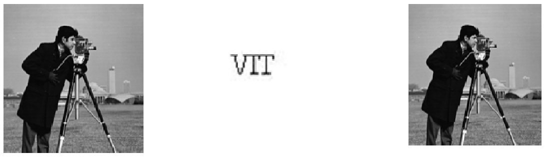
6.2 PERFORMANCE ANALYSIS OF USDNA

The cover image, watermark and the watermarked image are shown in Fig 6. From Fig.6 it is clear that the algorithm is imperceptible and the calculated PSNR shows that the watermarked image is of good quality when hidden in the low frequency channel than middle and the high frequency. The extracted watermark from all the three frequency band without any attack are shown Fig 7. In table 3 the extracted watermark after various attacks from all three frequency band are given with similarity measure NC.

In table 4 the peak signal to ratio (PSNR) and the similarity measure (NC) of the extracted watermark under normal condition is given. In table 5 the PSNR values of the extracted watermark after various attacks are shown. Each attack is tested by hiding information in all the three frequency level of an image. Table 6 shows that the watermark is hidden in low, middle and high frequency part of an image and the calculated PSNR values after each attack. The proposed algorithm USDNA resists salt and pepper noise, Gaussian noise and rotation attacks when watermark is hidden in low frequency part of an image than middle and high frequency components. The algorithm is not withstanding cropping and histogram equalization attack when information is hidden in the low frequency band but survives the attacks when information is hidden in the high frequency components.

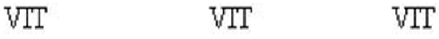
Table.4. PSNR and NC Values of the original and the watermarked image under normal conditions

Frequency Band	Low Frequency	Middle Frequency	High Frequency
PSNR	32.5311	30.5372	32.5267
NC	0.9935	0.9930	0.9935



a. Cover image b. Watermark c. Watermarked

Fig.6.



(a) Low Frequency (b) Middle frequency (c)High Frequency

Fig.7. Extracted Watermarks

Table.3. Calculated NC values of extracted watermark from the three frequencies band after various using USDNA

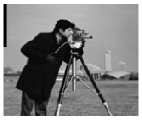
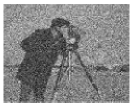
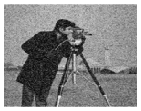
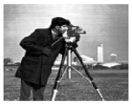
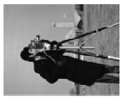
Watermarked Image With different attacks	Extracted watermark from low frequency	Extracted watermark from middle frequency	Extracted watermark from high frequency
			
cropping	NC = 0.8213	NC = 0.8514	NC = 0.8941
			
Gaussian Noise	NC = 0.9215	NC = 0.9212	NC = 0.9230
			
Salt and pepper (mean=0.2)	NC = 0.9501	NC = 0.8942	NC = 0.901
			
Histogram Equalization	NC = 0.9805	NC = 0.9912	NC = 0.9965
			
Rotation (90°)	NC = 0.9910	NC = 0.9435	NC = 0.9965

Table.5. calculated PSNR values after attacks when watermark is hidden in low, middle and high frequency bands

Attacks	PSNR	PSNR	PSNR
Salt & Pepper attack (Mean = 0.2)	31.1356	30.5212	30.4319
Gaussian Noise (Mean=0.01, Variance=0.5)	35.4231	34.1213	34.0019
Rotation(90 degrees)	28.1213	28.0009	28.1001
Cropping (200,200,12,12)	29.1214	30.1213	30.0090
Histogram Equalization	30.0090	30.1412	31.1070

7. CONCLUSION

In proposed algorithm the features of discrete wavelet transformation is combined with the DNA concepts. In this paper two algorithm have been proposed in which first algorithm named as CBDNA which is used to derive unique DNA watermark using the cover data itself. The second algorithm is named as USDNA in which the user specified input is converted into unique DNA sequence. In both algorithms the watermark is embedded in all the frequency bands to increase the robustness of the algorithm.

As per the results, the algorithm-I (CBDNA) is found to be robust against many attacks including salt and pepper noise, Gaussian noise, cropping and histogram equalization attacks. If watermark is embedded in high frequency components, the CBDNA withstands rotation attack also. After each attack the similarity of the original and extracted watermark is measured through NC and it shows that its quality is good as its value is above 90%. It could be used for image authentication.

The results of algorithm-II (USDNA) show that it is robust against attacks such as salt and pepper noise, Gaussian noise, cropping of an image. If watermark is embedded in high frequency components, the CBDNA withstands both rotation and histogram equalization attack. After each attack the similarity of the original and extracted watermark is measured through NC and it shows that its quality is good as its value is above 90%. It could be used for copy right protection of an image.

As information is hidden in all the frequency components if an image, the watermark is extractable with good quality after any attacks.

REFERENCES

[1] Mitchell D. Swanson, Mei Kobayashi, and Ahmed H. Tewfik, 1998, "Multimedia Data-Embedding and Watermarking Technologies", Proceedings of the IEEE Transaction, Vol.86, No. 6, pp.1064 – 1087.

[2] Darko Kirovski, Fabien A. P. Petitcolas, 2003, "Blind Pattern Matching Attack on Watermarking Systems", *IEEE* Transactions on Signal Processing, Vol. 51, No. 4, pp.1045–1053.

[3] Chi-Kwong Chan, L.M Cheng, 2004, "Hiding Data in Images by Simple LSB Substitution" Transaction on Pattern Recognition Society, Vol.37, No.3, pp. 469-474.

[4] Gehani A, Labean T H, Reif J H, 2002, "DNA-based cryptography, DIMACS Series in Discrete Mathematics and Theoretical Computer Science", Transaction on theoretical Computer Science, Science Direct, Vol. 287, No.1, pp.3-38.

[5] Mohamed Al Baloshi, Mohammed E. Al-Mualla, 2007, "A DCT-Based Watermarking Technique for Image Authentication", AICCSA, IEEE/ACS International Conference on Computer Systems and Applications, pp.754–760.

[6] Mohd Saufee, Muhammad, Zuwairie Ibrahim, Osamu Ono and Marzuki Khalid, 2005, "Direct-Proportional Length-Based DNA Computing Implementation for Elevator Scheduling Problem" in the proceedings of TENCON, IEEE, pp.21–24.

[7] Potdar, V.M, Han, S, Chang, E, 2005, "A survey of digital image watermarking techniques" in Industrial Informatics INDIN, proceedings of third IEEE International Conference, pp.709- 716.

[8] Sotirios A. Tsaftaris, Aggelos K. Katsaggelos, Thrasyvoulos N. Pappas and Eleftherios T. Papoutsakis, 2004, "DNA computing from a signal processing viewpoint", IEEE Signal Processing Magazine, Vol.21, No. 5, pp.100 – 106.

[9] Mohammad Aboofazeli Gabriel Thomas Zahra Moussavi, 2004, "A Wavelet Transform Based Digital Image Watermarking Scheme" in the proceedings of CCGEI 2004, CCGEI.

[10] Dominik Heider and Angelika Barnekow, 2007, "DNA-based watermarks using the DNA-Crypt algorithm", BMC Bioinformatics.

[11] Guangzhao Cui, Limin Qin, Yanfeng Wang, Xuncai Zhang, 2007, "Information Security Technology Based on DNA Computing", in the proceedings of IEEE International Workshop on Anti-counterfeiting, Security, Identification, pp 288 – 291.

[12] Sotirios A. Tsaftaris and A.K. Katsaggelos, 2005, "On Designing DNA Databases for the Storage and Retrieval of Digital Signals", in the proceedings of International Conference on Natural Computation, Vol. 3611, pp.1192-1201.

[13] Sotirios A. Tsaftaris, Aggelos K. Katsaggelos, Thrasyvoulos N. Pappas and Eleftherios T. Papoutsakis, 2004, "How Can DNA Computing be applied to Digital Signal Processing?", IEEE Signal Processing Magazine, Vol.21, No.6, pp.57 – 61.

[14] Zaboli, S. Moin, M.S., 2007, "A Non-Blind Adaptive Image Watermarking Approach Based on Entropy in Contourlet Domain", IEEE International Symposium, pp 1687-1692.

[15] Gabriel Peterson, "Arnold's Cat Map".

[16] L. M. Adleman, 1994, "Molecular computation of solutions to combinatorial problems", Science Mgazine, Vol.266, No.5187, pp.1021-1024.