VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

CYBER SECURITY

J-COMPONENT FINAL REVIEW

TITLE: **CTS IMAGE WATERMARKING BASED ON DWT**

TEAM MEMBERS:

Y.ASHOK REDDY - 18BCE0120
CH.MANISH GUPTA - 18BCE0455
R.PHANIDHAR REDDY - 18BCE0175

UNDER THE GUIDENCE OF:-

DR. MURUGAN K

ABSTRACT:

Image watermarking is a technique to authenticate the user files by embedding and hiding digital code behind an image. For clearing the cheque rapidly, CTS is used. The digital cheque images are transmitted through Internet. It is normally considered that the system is safe and secure. But in practical, the intruders may damage the quality of cheque image or duplicate the cheque image. In order to maintain security and copyright protection, image watermarking is a powerful technique for this purpose based on DWT & DES. The proposed project provides high robustness, effectiveness and imperceptible to the watermarked image and achieves high PSNR value. In addition to this, it can also protect the content even after decryption is done.

An efficient digital watermark embedding algorithm for color image, which is based on the discrete wavelet transform (DWT) and the spectral characteristics of human vision system. Firstly, three color separations was performed for color image, and color components of color image were transformed by DWT. Secondly, the embedding position of the watermark was confirmed by comparing the energy value of the low frequency sub-band in the transformed blue component and green component. Thirdly, the watermark was made Arnold Transform for encryption and was embedded in the color component with a larger power. The simulation results showed that the embedded watermark had good invisibility and robustness for the common image processing, such as filtering, noise, especially compression and cropping.

KEYWORDS:

CTS :- Cheque Truncation System

DWT:- Discrete Wavelet Transform

DES :- Discrete Encryption Standard

PSNR:- Peak Signal to Noise Ratio

MSE :- Mean Squared Error

INTRODUCTION:

With the advent of Internet technology, the protection of intellectual property rights has become progressively important. The information includes images, audio, image, or text are stored and transmitted in a digital format can be easily copied without any loss of quality. Digital watermark is introduced to solve this problem. Digital watermarking is a technique to authenticate the user files by embedding and hiding digital code behind an image. Then the digital content can be exchanged over the Internet over peer-to-peer networks. This has caused major concerns to those content providers who produce these digital contents. In order to maintain the digital watermarking method to be effective, it should be unobserved and robust to common image attacks like compression, filtering, rotation, scaling cropping, and collusion. The watermarking can be done in 2 ways.

They are: 1. SPATIAL DOMAIN TECHNIQUE
2. FREQUENCY DOMAIN TECHNIQUE

1. **SPATIAL DOMAIN TECHNIQUE** :-
   In this technique, watermark is embedded by directly changing the pixel values of the host image [1]. This method is very simple. These methods are commonly used in video watermarking where the prime concern is realtime performance. The resulting watermark may or may not be perceptible, depending upon the intensity value. Some methods of watermarking in spatial domains are Correlation Based techniques, least significant bit modification (LSB), and Predictive coding scheme.

2. **FREQUENCY DOMAIN TECHNIQUE :-**
   In this technique, altering the transform coefficients of the frames does embedding of the watermark. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are most commonly used transforms. The watermark is embedded into the original image. Initially, the host image is converted into a frequency domain by transformation techniques. Then, the transformed coefficients are changed to store the watermark information. At last, the watermarked image is obtained by applying the inverse transform. Due to its multiresolution characteristics, a number of researchers concentrated on using DWT. It provides both spatial and frequency domain characteristics thus making it compatible with the Human Visual System (HVS). Moreover, DWT can be combined with other algorithms to enhance robustness and invisibility.

LITERATURE REVIEW :-

1. **Bhatnagar & Raman (2009)(ELSEVIER):** presented a new semi-blind reference watermarking scheme based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for copyright protection and authenticity. A grey scale logo image is used as watermark instead of randomly generated Gaussian noise type watermark. For watermark embedding, the original image is transformed into wavelet domain and a reference sub-image is formed using directive contrast and wavelet coefficients. Watermark is embedded into reference image by modifying the singular values of reference image using the singular values of the watermark. A reliable watermark extraction scheme is developed for the extraction of watermark from distorted image.

2. **Rani et al. (2015)(ELSEVIER):** proposed two schemes; the basic idea behind both the schemes is making use of Discrete Wavelet Transformation and Singular Value Decomposition to extract robust features of host image. The first approach consists of dividing the host image into overlapping sub images of size 8 × 8. Each block is further decomposed up to level-one using Discrete Wavelet Transform followed by Singular Value Decomposition. In the second approach the image is first subject to DWT, then the approximation part is chosen and later it is divided into overlapping sub-images of size 4 × 4.

3. **Nematollahi et al. (2015)(ScienceDirect):** presented a new blind digital speech watermarking technique based on Eigen-value quantization in Discrete Wavelet Transform. Initially, each frame of the digital speech was transformed into the wavelet domain by applying Discrete Wavelet Transform. Then, the Eigen-value of Approximation Coefficients was computed by using Singular Value Decomposition. Finally, the watermark bits were embedded by quantization of the Eigen-value.

4. **Mishra et al. (2014)(MDPI)** presented an optimized watermarking scheme based on the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The singular values of a binary watermark are embedded in singular values of the LL3subband coefficients of the host image by making use of multiple scaling factors. The multiple scaling factors are optimized using a newly proposed Firefly Algorithm having an objective function which is a linear combination of imperceptibility and robustness. The embedding algorithm is robust against common image processing operations.

5. **Jane et al. (2014)(ScienceDirect)** presented a hybrid non-blind scheme based on DWT and Singular Value Decomposition (SVD). After decomposing the cover image into four sub bands (LL, HL, LH and HH), SVD is applied to LL band and modify diagonal singular value coefficients with the watermark itself by using a scaling factor. Finally, LLband coefficients are reconstructed with modified singular values and inverse DWT is applied to obtain watermarked image.

6. **Bin (2011)(ELSEVIER):** proposed a novel digital watermarking scheme based on Discrete Wavelet Transform (DWT). The theory of digital watermark based on DWT for electronic seal is discussed. The digital watermark is scrambled with logistic chaotic sequences to improve the security of the system. Then the watermark signals are converted into a binary sequence embedded to the high (HL and HH) frequency band of the document in DWT domain. The algorithm of how to embed and extract the watermark is shown in the paper. Image quality is checked with a number of widely used parameters such as PSNR, Normalized Correlation and JPEG compression.

7. **P. Kulkarni, Shraddha Bhise, S. Khot:** Published Watermarking is delicate to various attacks in spatial domain, Hence in most of the watermarking technique's transform domain is used. This paper takes a

survey of such digital watermarking techniques and methods like Discrete cosine transform (DCT), Singular value decomposition (SVD), SVDDCT, DWT-SVD with different approaches along with their applications, advantages and disadvantages. Further future work and implementation plan is also mentioned in the paper. KeywordsDiscrete Wavelet transform (DWT), SVD.

8. **C. Rajeev, K. P. Girish:** Published Watermarking is the technique to insert some kind of ownership information in any digital media like image, audio, or video. This enables the owner of the media to claim the ownership against any illegal use or claim of false ownership. In this paper, the watermarking is performed with gray image in transform domain to compare discrete wavelet transform (DWT) and discrete Mojette transform based on the quality measures like peak signal-to-noise ratio (PSNR) and mean square error (MSE). The proposed work also deals with a review of

   the various attacks on the watermarked image to alter the watermark, to remove, and to degrade the quality of the watermark in both cases.

9. **Jiang Qine-feng, Qian Gong :** Published Digital watermarking (DW) is a technology that hides information in image to provide authentication. Information hiding is done by the tampering content of the image. In this research, self image embedding using two level discrete wavelet transform (2DWT) with singular value decomposition (SVD),and probabilistic neural network (PNN) classifier method. Firstly, take cover image and create watermark image using bi-cubic interpolation method.Secondly, encrypt watermark image using stream cipher (SC) method. Thirdly, the watermarking embedding region is directed with 2DWT and the low frequency DWT coefficient is isolated into noncovering pieces; SVD is connected to each block.

10. **Guangmin Sun, Yao Yu:** Published The efficiency of digital watermarking algorithm is based on robustness of embedded watermark against various attacks.With the use of Internet technology,it is easy to copy the digital products such as text, digital audio, image, video.Therefore digital product must be secured . Many methods are available for protecting digital data. A method is used to improve the ownership over image by placing low level signal directly into image; this signal is called as watermark.

11. **Kundar D,hotzinakos:** Published Research in the area of digital watermarking has focused primarily on the design of robust techniques for the copyright protection of multimedia data. In such methods a watermark is imperceptibly embedded in a host signal such that its removal using common distortions on the marked signal is difficult without degrading the perceptible data content itself. Watermarking can also be used to address the equally important, but underdeveloped, problem of tamper proofing.As a great deal of multimedia is stored in digital format, it has become easier to modify or forge information using widely available editing software.

12. **JAYPRAKASH UPADHYAY, Dr. BHARAT MISHRA, Dr. Prabhat**

Patel: Published The color watermarked image is obtained & watermark can easily be extracted in both clean and noisy environments. Experiments are performed to verify the robustness of the proposed algorithm. The result shows that the proposed algorithm is better than other existing algorithms in terms of providing a high PSNR. It is also shown that the proposed algorithm is highly robust against various kinds of attacks such as noise, filtering, cropping & rotation.

13.**Shanshan Zhang,Xiaohong Wang,Shizheng Zhou:** Published The image watermarking technology is an important aspect about multimedia authentication and copyright protection, in order to enhance its reliability and security, this paper proposes an encryption algorithm based on color image watermarking in security DCT domain. By processing the color watermark image's R, G, B pixels, that is, converts the pixel value matrix into binary one-dimensional sequence, then get the one-dimensional sequence as the watermark embedding the carrier images, overcame the traditional understanding defects about the DCT domain can only be embedded two value image.

14.**J.Antonino-Daviu:** Published The discrete wavelet transform (DWT) is an ideal tool for this purpose, due to its suitability for the analysis of signals whose frequency spectrum is variable in time. The paper shows how the study of the high-level signals resulting from the DWT of the transient starting current of an induction motor allows the detection of a particular characteristic harmonic that occurs when a rotor bar breakage has taken placethe application of the DWT for broken bar detection is optimized, regarding certain parameters of the transform such as type of the mother wavelet, number of decomposition levels, order of the mother wavelet and sampling frequency.

15.**PAVEL RAJMIC,ZDENEK PRUSA:** Published The paper presents a detailed analysis of algorithms used for the forward and the inverse discrete wavelet transform (DTWT) of finite-length signals.The paper provides answers to questions such as "how many wavelet coefficients are computed from the signal at a given depth of the decomposition" or conversely, "how many signal samples are needed to compute a single wavelet coefficient at a given depth of the decomposition" or "how many coefficients at a given depth are influenced by the selected type of boundary treatment" or "how many samples of the input signal simultaneously influence two neighboring wavelet coefficients at a given depth of the decomposition".

PROBLEM STATEMENT:

For clearing the checks rapidly, CTS(Check Truncation System) of bank transmits the digital image of check to the drawee bank. The intruder may damage or duplicate the image and may misuse it. The proposed project is about the security and copyright protection of the digital image of check.

OBJECTIVE:

To embed the watermark in digital image of check which is not perceptible to Human eyes as to authenticate the user. Also to extract the watermark at the receiver's end.

PROPOSED TECHNIQUES:

Arnold transform of the watermark image N*N

Before the watermarking image is embedded, it should be encrypted in advance, namely made the scrambling transformation in order to ensure the security of the watermarking information and improve the robustness of the original image.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = C \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \qquad x, y \in (0,1,2, \ldots, N-1) \qquad (1)$$

TECHNIQUES:

1. **DISCRETE WAVELET TRANSFORM (DWT):**
   Discrete Wavelet Transform is a time/frequency analysis algorithm which has the characteristic of multi-resolution analysis. It not only analyzes signals in the time domain or frequency domain but in the combined domain with time and frequency so that the signal has a good frequency resolution in the low frequency sub-band and a good time resolution in the high frequency subband.

   Discrete Wavelet Transform for two-dimensional image is to perform multi-resolution decomposition for the image, which decomposes the image into the low frequency sub-band and the high frequency sub-band whose resolutions are different. The main energy of the image is accumulated in low frequency sub-band where records the feature information of the image.

The low frequency sub-band is the best approximation to original image with maximum scale and minimum resolution after wavelet transformed. The high frequency sub-band including horizontal, vertical and diagonal contains less energy and its sub-band records the image's details and texture information.

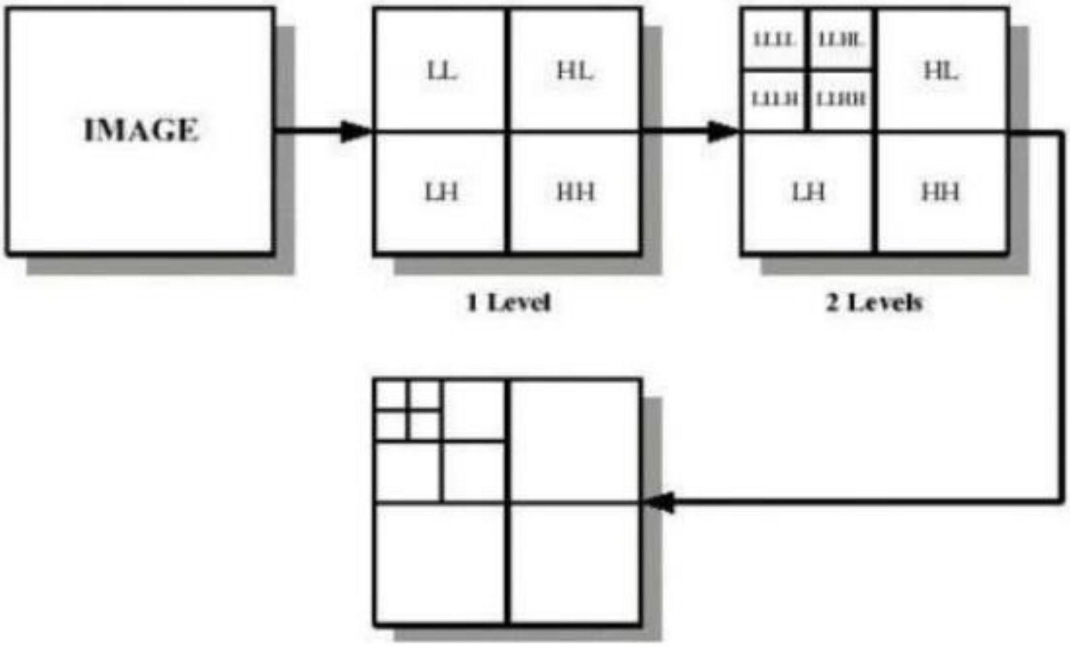
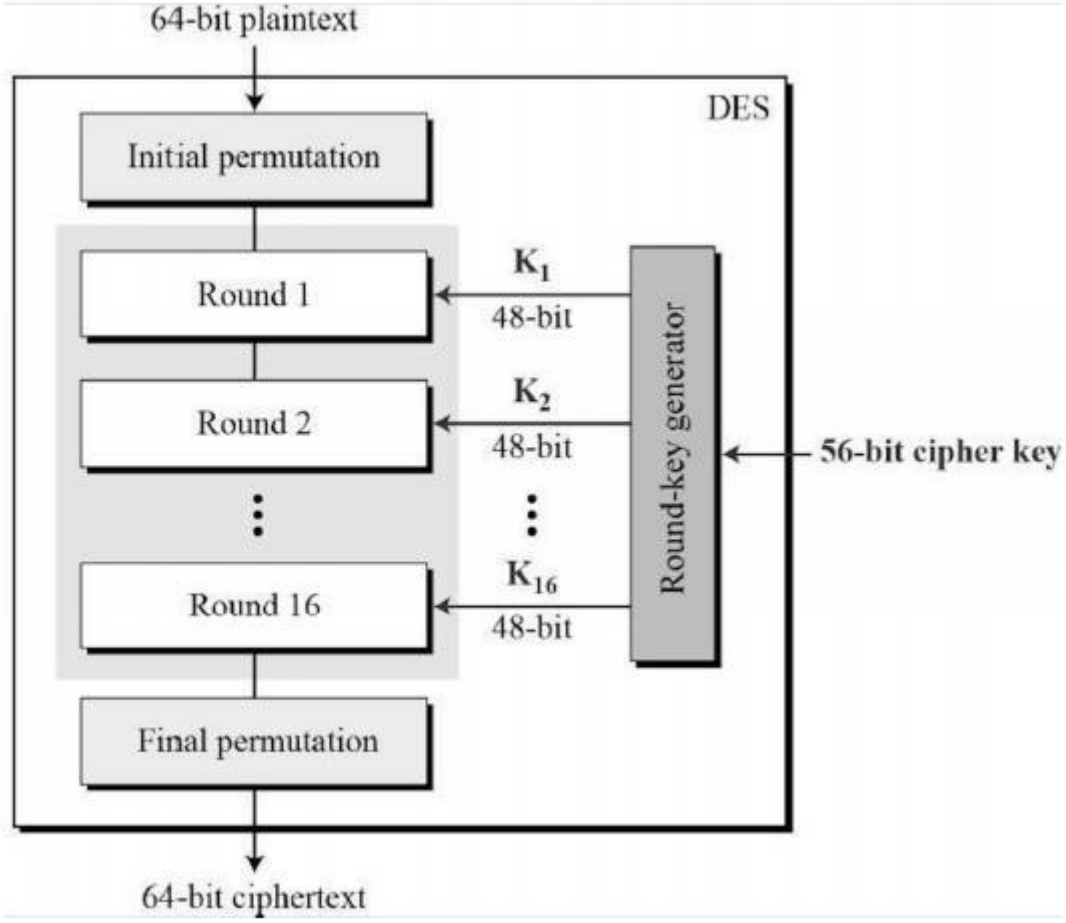


Image compression levels

2. **DATA ENCRYPTION STANDARD (DES):**
The Data Encryption Standard (DES) is a symmetric-key block cipher, which uses 16 rounds of permutation [12]. At the encryption side, DES takes a 64-bit plaintext and creates a 64-bit cipher text. At the decryption side, DES takes a 64-bit cipher text and creates a 64-bit block of plaintext. The same 56-bit cipher key is used for both encryption and decryption. DES operates on 64-bit block of plaintext. After initial permutation, the block is divided into right half and left half of each having 32-bits long. Then there are 16 rounds of identical operation, called function(f), in which the data are combined with the key. After sixteenth round, the right and left halves are joined and a final permutation (inverse of initial permutation) finishes off the algorithm.

The same key is used for both encryption and decryption. In each round, the key bits are shifted and then 48 bits are selected from the 56 bits of the key.



DES operation

3. WATERMARKING EMBEDDING PROCESS:

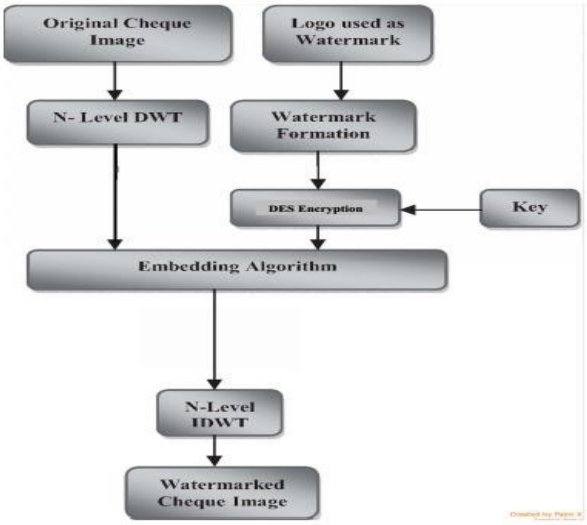
This algorithm starts with choosing original image and the watermark image. A two dimensional image is transformed into single DWT; image is decomposed into four parts. Top left block is a low frequency of original image, bottom left block contains the vertical details of the original image, the top right block contains horizontal detail of the image and the bottom right block contains high frequency of original image. To achieve 3-level DWT, same process is repeated for twice. The low frequency coefficient contains more information of the original image, so it provides high robust to embed watermark in this position. Watermark must be robust against compression so it is necessary to choose the low frequency of image to embed watermark. A binary image is used for the watermark. This digital image is divided into blocks of size 8X8. DES is applied on all these 64 bit blocks of binary watermark image with a same key. DES encrypted blocks are assembled to generate the watermark. In the proposed scheme DES is used to assure security to the watermark image. Block wise DES encryption ensures the effectiveness of the encryption method. Same 64bit binary key has to be used for encryption and decryption.

Steps Followed In Embedding Process:

Step 1: Decompose the original image I (NXN) by 3-level DWT.
Step 2: Generate random key K of 64 bits.
Step 3: Divide the binary watermark image of size ((NXN)/4) in Block size8X8.
Step 4: Encrypt the image blocks with DES using key K.
Step 5: Generate encrypted image W*.
Step 6: Calculate PSNR & MSE value.

4. WATERMARKING EXTRACTION PROCESS:

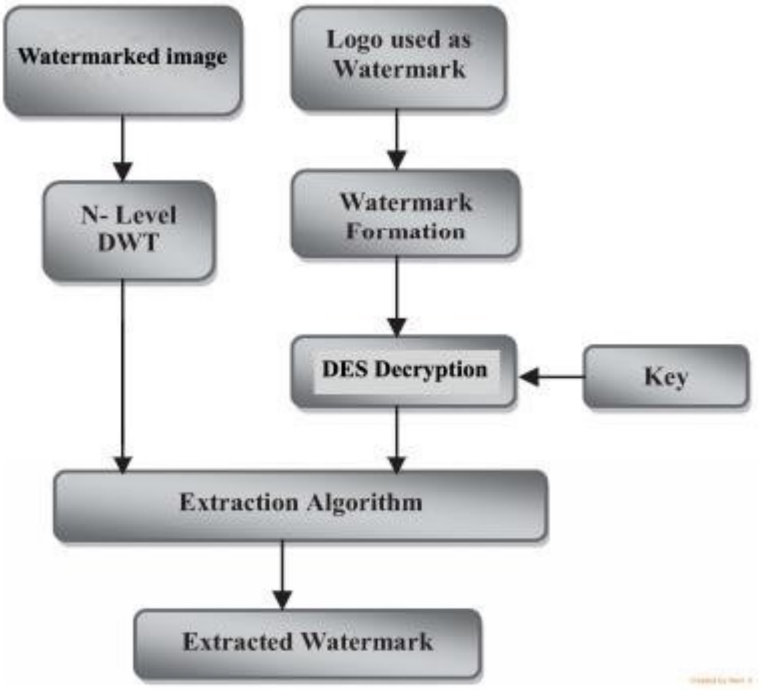
To extract the watermark image, the secret Key is obtained. Embedding coefficient also plays an important role to extract the watermark of satisfying visual quality. Similar to the embedding process, before extracting the watermark, the system needs to extract the cheques image by using 3-Level DWT and 64-Bit DES.



Flowchart of Watermarking Embedding Process

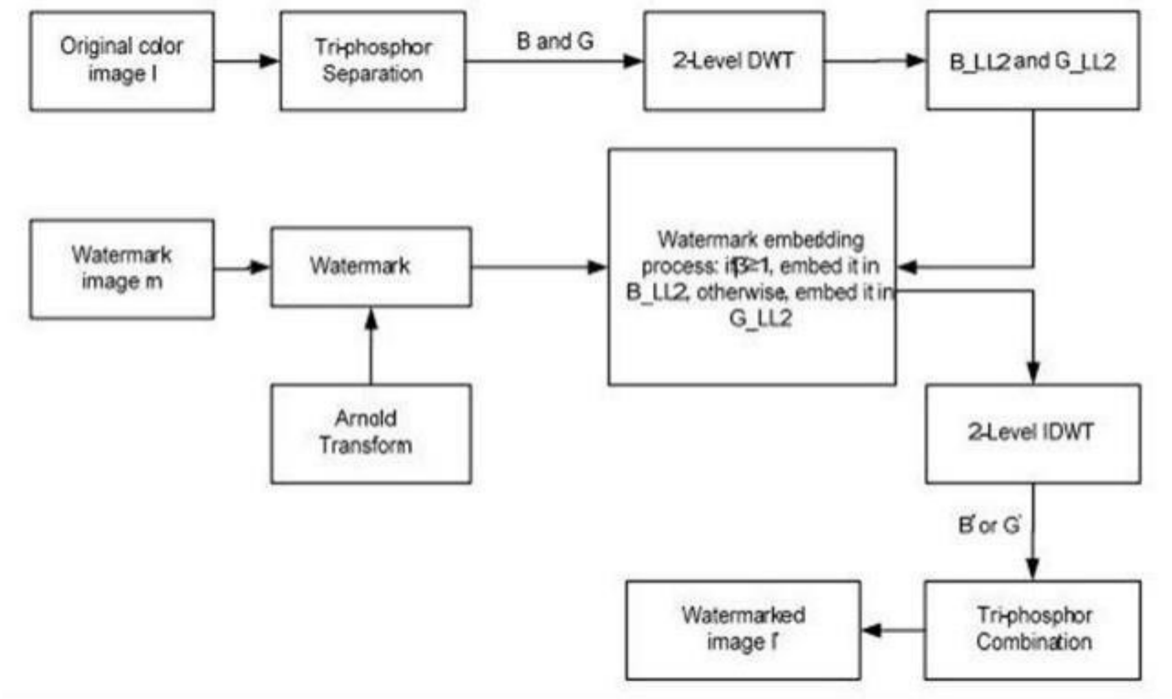
Steps Followed In Extraction Process:

Step 1: Inverse Transform to the watermarked image by three levels IDWT.
Step 2: Choosing LL band coefficient of 3-Level IDWT in watermarked image.
Step 3: Divide the encrypted image W* in blocks of size 8X8.
Step 4: Decrypt the image blocks with DES using key K.
Step 5: Generate watermark image and original image. **Step 6**: Calculate PSNR and MSE value.



Flowchart for watermarking embedding process

FLOWCHART:



ALGORITHM

Step 1 : Reading the cover image and watermark image.

Step 2 :Converting the watermark image to gray level scale.

Step 3: Decomposition of the image into red, green and blue component.

Step 4: Applying 2-level Discrete Wavelet Transform on green and blue component.

Step 5: Calculating the energy of second low frequency subband of the green and blue component of image. **Step** 6: Calculating the value of Beta.

Step 7: If the value of Beta is greater than or equal to one than the watermark will be embedded in second low frequency subband of blue image component of the image.

Step 8: Embedding the watermark in the selected subband.

Step 9: Applying the 2-level Inverse Discrete Wavelet Transform on the component where the watermark is embedded.

Step 10: Combining the three components of image to get the resultant watermarked image.

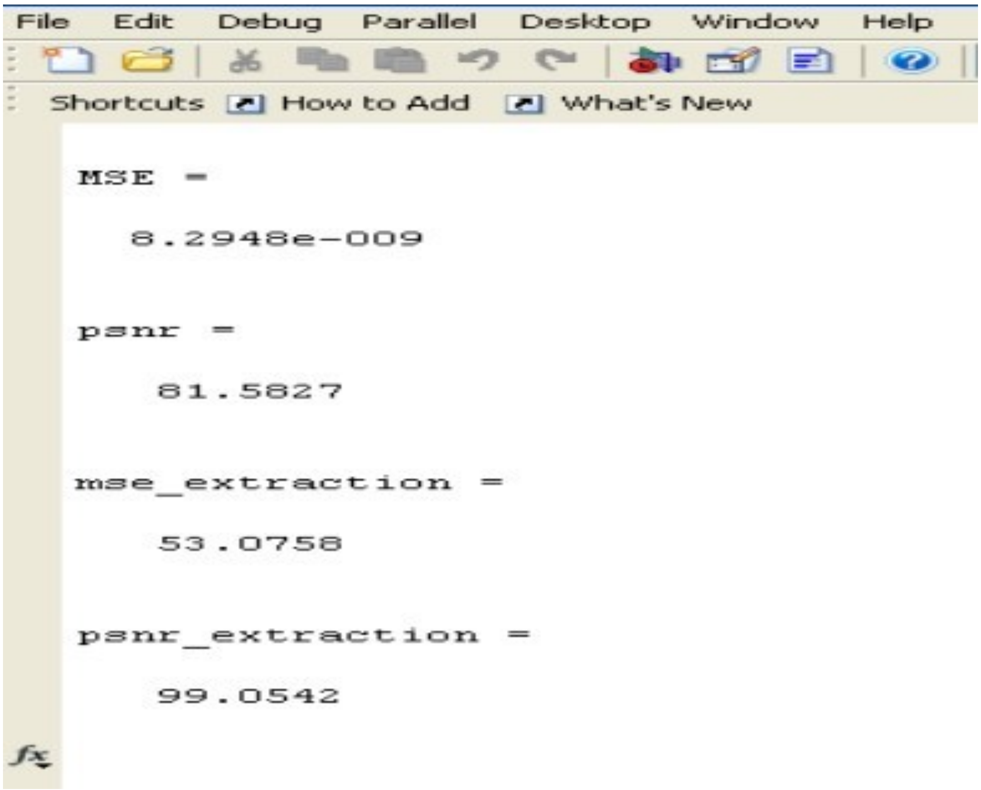
PERFORMANCE EVALUATION:

$$\text{MSE}=\frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M*N},$$

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

By calculating MSE and PSNR values, the quality of the image can be measured. Higher the PSNR value, higher its quality.

We have got the PSNR value as 81.582.It means that the quality of the watermarked image is good.



```
MSE =

  8.2948e-009


psnr =

   81.5827


mse_extraction =

   53.0758


psnr_extraction =

   99.0542
```

HOW TO EXECUTE THE PROGRAM IN MATLAB:

Step 1: Open program file.

Step 2: Run the program.

Step 3: Select the cover image (cheque image).

Step 4: Select the watermark image (logo, symbol).

Step 5: Perform 3-level DWT on cover image.

Step 6: Select “show final watermarked image” in the menu.

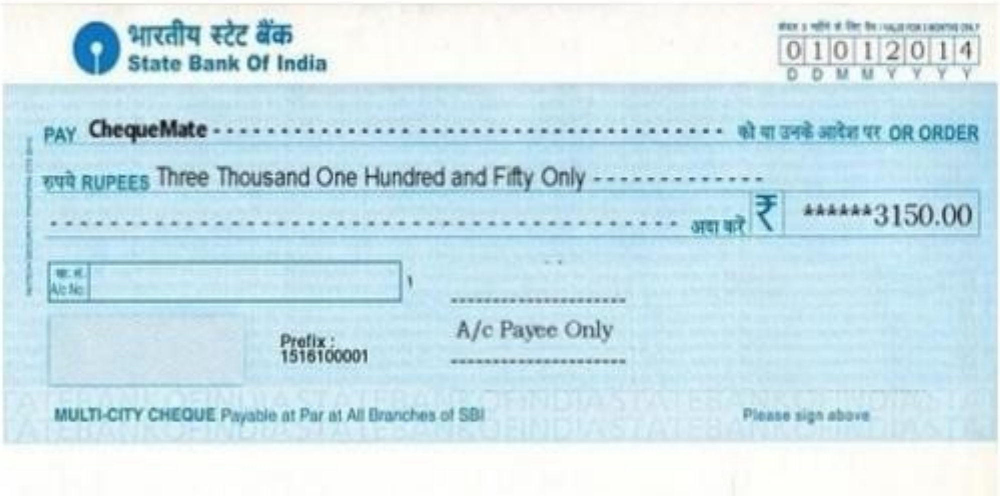
Step 7: Select DES encryption to encrypt the image.

Step 8: After completingthe watermark embedding process, the cheque is transferred to drawee of the other branch.

tep 9: After receiving the cheque image from the sender, with the help of DES decryption algorithm, the watermarked cheque image is decrypted.

Step 10: Select "Show extracted image" in the menu.

Step 11: Calculate MSE & PSNR values using below equations.



भारतीय स्टेट बैंक
State Bank Of India

केवल 3 महीने के लिए वैध / VALID FOR 3 MONTHS ONLY

0 1 0 1 2 0 1 4
D D M M Y Y Y Y

PAY ChequeMate .... को या उनके आदेश पर OR ORDER

रुपये RUPEES Three Thousand One Hundred and Fifty Only ....

.... अदा करें ₹ ******3150.00

खा. सं.
A/c No

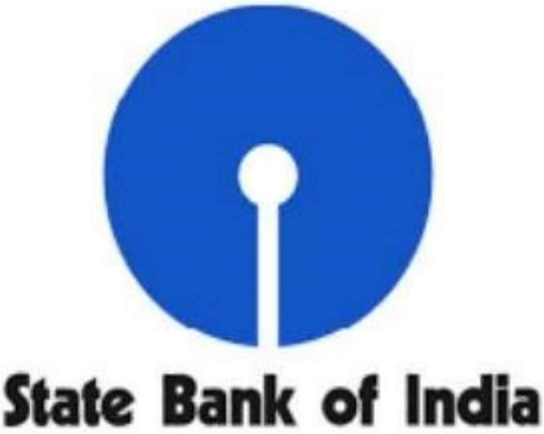
Prefix :
1516100001

A/c Payee Only

MULTI-CITY CHEQUE Payable at Par at All Branches of SBI

Please sign above

COVER IMAGE (CHEQUE)



WATERMARK IMAGE

RESULTS:

This is the watermark inserted image to verify original cheque or not

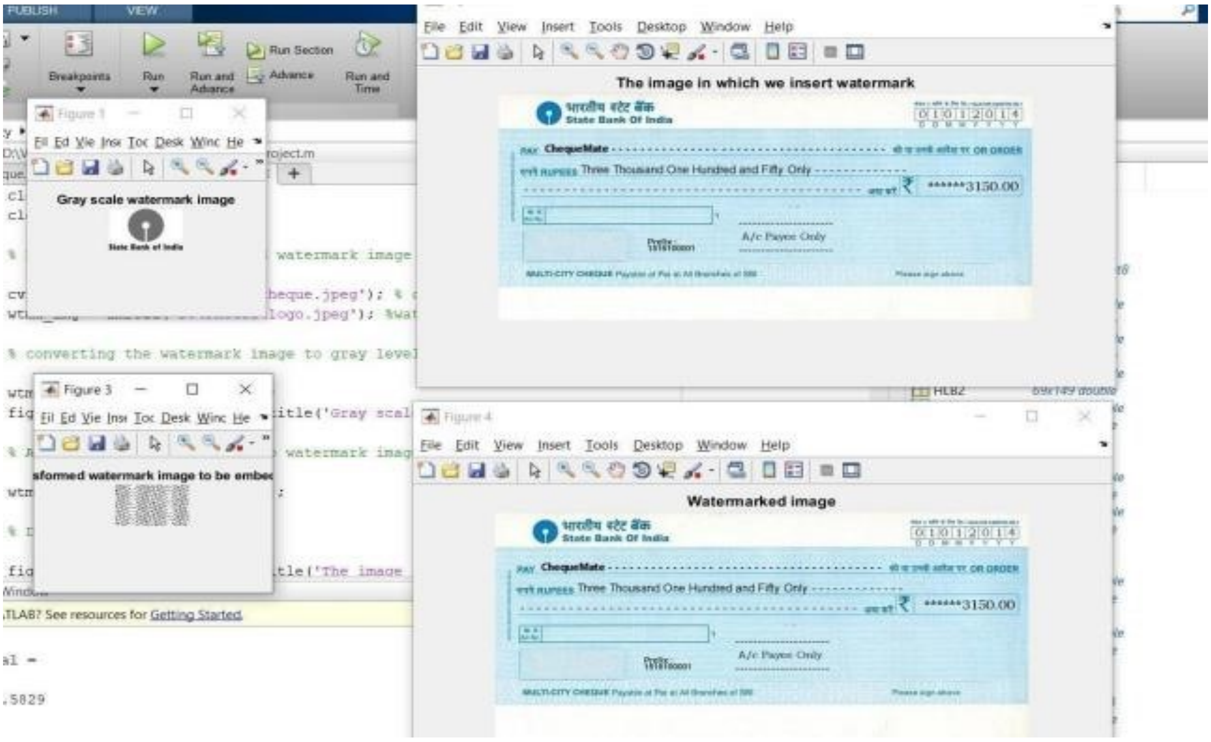


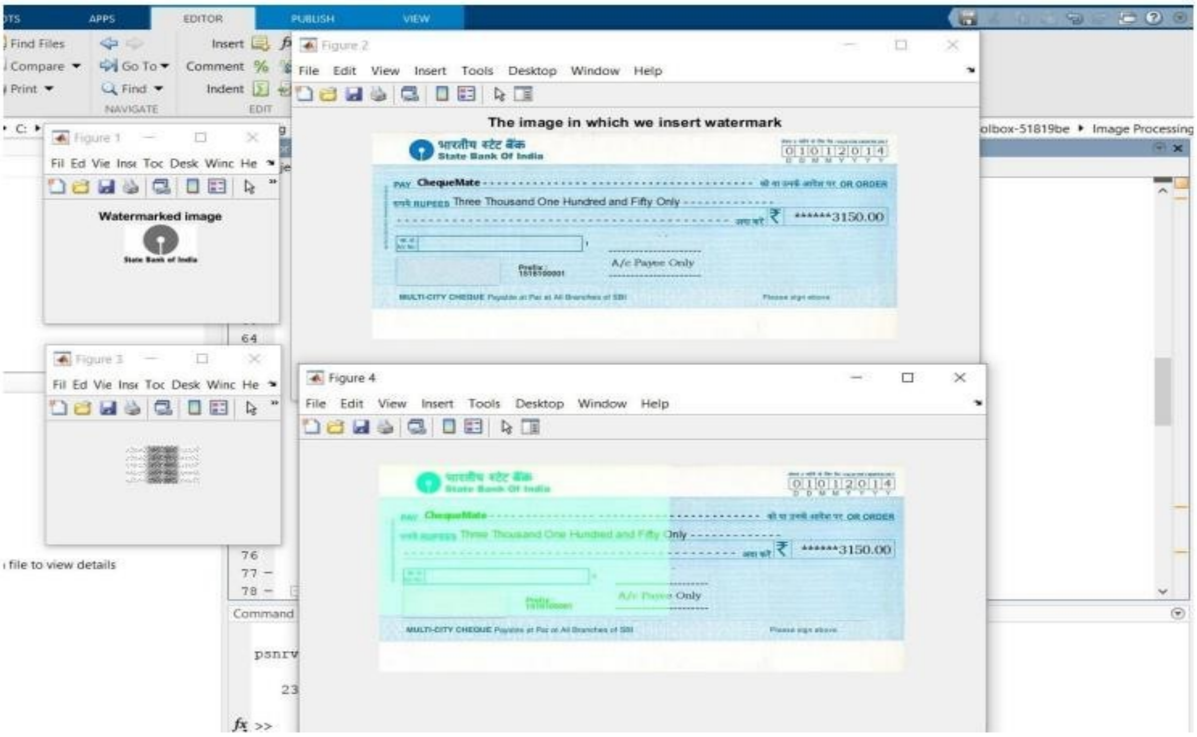
Figure 1
Gray scale watermark image
State Bank of India
Figure 3
sformed watermark image to be embe
The image in which we insert watermark
Figure 4
Watermarked image
भारतीय स्टेट बैंक
State Bank Of India
PAY ChequeMate
Three Thousand One Hundred and Fifty Only
******3150.00
A/c Payee Only
MULTI-CITY CHEQUE
TLAB? See resources for Getting Started.

```
cl
cl
%                               watermark image
cv                              heque.jpeg'); % c
wt                              logo.jpeg'); %wat
% converting the watermark image to gray level
wtr
fig                             title('Gray scal
%                               watermark imag
wtr                             ;
%
fig                             tle('The image
```

```
al =
.5829
```

By changing the 'alpha' and 'beta' values the scanner which is used to scan theCTS image,detect the original image of the cheque.

The below img shown in this project detect the place where the watermark hasbeen inserted.



```
psnrv
    23
fx >>
```

CONCLUSION:

This method is used to identify the valid cheque issued by the bank to particular customers and reduces the fake cheque transactions. And also make the bank employees to identify the valid cheque through this quick process.

Identical frame based image-watermarking technique on 3-level DWT and DES is proposed which is perceptually invisible. The experimental results show that high robustness over various attacks and imperceptibility to the cheque image. This provides security, copyright protection and data authenticity to cheque image. In future our plan is to minimize the watermark embedding time to improve the performance of the proposed system.

REFERENCES:

1. *Snehakadu, Ch.Naveen, V.R. Satpute, A.G. Keskar, "DWT based video watermarking technique", IEEE 2016.*

2. *MeetaMalonia, Surendra Kumar Agarwal, "Digital Image Watermarking using Discrete Wavelet Transform and ArithmeNc Progression Technique", 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science.*

3. *SudhanshuSuhasGonge, Prof.Ashok A.Ghatol,"Combined DWT-DCT Digital watermarking technique soRware used for CTS of Bank", ICICT 2014.*

4. *PinkiTanwar, ManishaKhurana, "Improved PSNR and NC in Digital Image Watermarking Using RDWT and SVD", InternaNonal Journal of Advanced Research in Computer Science and SoRware Engineering, Volume 6, Issue 5, May 2016.*

5. *Mohammed Al Baloshi, Mohammed E.AlMullala, "DCT based technique for image authenNcaNon", IEEE 2015.*

6. *NirupmaTiwari, Manoj Kumar Ramaiya, Monika Sharma, "Digital Watermarking using DWT and DES", IEEE 2012.*

7. *PravinM.Pithiya, H.L.Desai, "DWT based digital watermarking, dewater-marking and authenNcaNon", IJERD 2013.*

8. *Kuo-Cheng Liu, "Human Visual System based watermarking for colorimage", IEEE 2009.*

9. *S. Islam, R. Debnath, and S. Hossain, "DWT based digital watermarking technique and its robustness on image rotaNon, scaling, jpeg compression, cropping and mulNple watermarking", mar. 2007, pp. 246 –249*

10. *S SBedi, Ashwanikumar and PiyushKapoor, "Robust secure SVD based DCT-DWT oriented watermarking technique for image authenNcaNon", IEEE 2009.*

11. *Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Department of Computer Engineering, School of Electrical Engineering, Princess Sumaya University for Technology, Jordan Journal of Computer Science 3 (9): 740- 746, 2007 ISSN 1549-3636 © 2007 Science PublicaNons.*

12. *Jiang Qine-feng, Qian Gong, "A new Image EncrypNon Scheme Based on DES", IST 2009 – InternaNonal Workshop on Imaging Systems and Technology Shenzhen, China, IEEE 2009.* **[13]** *TamanaTabasum,S.M.MohidulIslam,"Digital video watermarking technique based on idenNcal frame extracNon in 3- level DWT", IEEE 2012.*

14. *Wang.S and Y. Lin, "Wavelet Tree QuanNzaNon for CopyrightProtecNon*

Watermarking", IEEE Trans. Image Processing, vol 13, no.2,pp: 154-164.

15. *Mei Jianshengl, Li Sukangl and Tan Xiaomei2, "A Digital Watermarking Algorithm Based On DCT and DWT", Nanchang Power Supply Company, Nanchang, China Proceedings of the 2009 InternaNonal Symposium on Web InformaNon Systems and ApplicaNons (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107.*

16. *AmanpreetKaur, Dr. Naresh Kumar Garg, "An Improved Watermarking of Digital Images using DWT & SVD Approach",InternaNonal Journal of Advanced Research in Computer and CommunicaNon Engineering Vol. 5, Issue 11, November 2016.*

17. *Guangmin Sun, Yao Yu, "DWT based watermarking algorithm of color image" IEEE 2007.*

18. *PraNbha Sharma, ShanN Swami, Published 2013,MathemaNcs, "Digital Image Watermarking Using 3 level Discrete Wavelet Transform", semanNcscholar:Corpus ID:62884970*

19. *Wang Huai-bin, Yang Hong-liang, +1 author Wang Shao-ming, Computer Science 2010 InternaNonal Conference on Electrical and Control Engineering,"A New*

Watermarking Algorithm Based on DCT and DWT Fusion", Published 2010 researchgate.

20. *R. Kishore, Sunesh, Computer Science World Academy of Science, Engineering and Technology, InternaNonal Journal of Computer and InformaNon Engineering. Published 2016 researchgate.*

CODE:

```
 clc

clear all

% Reading the cover image and watermark image  cvr_img              =           imread('D:

\Photos\cheque.jpeg');           %          cover  image  wtmk_img  = imread('D:

\Photos\logo.jpeg'); %watermark image % converNng the watermark image to gray level

scale

wtmk_img = rgb2gray(wtmk_img);
figure(1); imshow(wtmk_img); Ntle('Gray scale watermark image');
% Applying Arnold Transform to watermark image wtmk_img

= arnold(wtmk_img,20);

% Displaying Image

figure(2); imshow(cvr_img); Ntle('The image in which we insert watermark');
figure(3); imshow(wtmk_img); Ntle('Transformed watermark image to be embedded');

% DecomposiNon of red, green and blue component of the image

rmat = cvr_img(:,:,1); % matrix of the red component
                      gmat = cvr_img(:,:,2); % matrix of the green component


bmat = cvr_img(:,:,3); % matrix of the blue component  %

2-level Discrete Wavelet Trasform on green component

[LLG1, HLG1, LHG1, HHG1] = dwt2(gmat, 'haar');
[LLG2, HLG2, LHG2, HHG2] = dwt2(LLG1, 'haar');
```

```
% 2-level Discrete Wavelet Trasform on blue component

[LLB1, HLB1, LHB1, HHB1] = dwt2(rmat, 'haar');

[LLB2, HLB2, LHB2, HHB2] = dwt2(LLB1, 'haar');

% CalculaNng the energy of LLG2

[LL2row, LL2col] = size(LLB2); % or [LL2row, LL2col] = size(LLG2)

sum_LLG2 = 0;
        for i = 1:LL2row
               for j = 1:LL2col
               sum_LLG2 = sum_LLG2 + (LLG2(i,j))^2;
       end
end
                LLG2en = sum_LLG2/(LL2row * LL2col);
sum_LLB2 = 0;
        for i = 1:LL2row
               for j = 1:LL2col
                sum_LLB2 = sum_LLB2 + (LLB2(i,j))^2;
                          end
                 LLB2en = sum_LLB2/(LL2row * LL2col);

% calculaNon of beta

bet = LLB2en/LLG2en;

% SelecNon of low frequency

subband If bet>=1 sLL2=LLB2; alp=0.1

comp =”blue”;  else  sLL2=LLG2;

alp=8;  comp=”green”; end

% Embedding watermark in the selected subbat

wtmk_img = im2double(wtmk_img);
        for i = 1:50 for
                j = 1:82
                 sLL2(i,j) = sLL2(i,j) + alp*wtmk_img(i,j);
                   end end

% 2-level Inverse Discrete Wavelet Transform on the selected component
```

```
if comp == "blue"
LLB1 = idwt2(sLL2, HLB2, LHB2, HHB2, 'haar');


LLB2(:,298) = [];
webc = idwt2(LLB1, HLB1, LHB1, HHB1, 'haar');


webc(276,:) = [];
        else

LLG1 = idwt2(sLL2, HLG2, LHG2, HHG2, 'haar');

LLG1(:,298) = [];
                 wegc = idwt2(LLG1, HLG1, LHG1, HHG1, 'haar');
                          wegc(276,:) = [];
                                wegc = uint8(wegc);
                                 end

% ResulNng watermarked image  if comp ==

"blue"  wtmked_img_mat = cat(3, rmat, gmat,

webc);

        else

        wtmked_img_mat = cat(3, rmat, wegc, bmat);               end

       figure(4); imshow(wtmked_img_mat); Ntle('Watermarked image');
        %Performance EvaluaNon Indexes of the Algorithm  psnrval

        = psnr(wtmked_img_mat,cvr_img)

        %Arnold transform

        funcNon
        y=arnold(im,num) [rown,coln]=size(im);
        for
        inc=1:num for row=1:rown
for col=1:coln nrowp = row;

ncolp=col; for ite=1:inc newcord =[1 1;1 2]*[nrowp ncolp]';

                nrowp=newcord(1);

ncolp=newcord(2);

end
```

```
newim(row,col)=im((mod(nrowp,rown)+1),(mod(ncolp,coln)+1));
  end end end                                               y=newim;
                                                            end
```