COMPARATIVE STUDY OF VARIOUS WATERMARKING TECHNIQUES

PRITHESH S
UNDER GUIDANCE OF PRADEEPA M
Vellore Institute of Technology
Vellore, India
prithesh07@gmail.com

Abstract- **In the present era, technology has developed enormously with respect to time and it's still growing. Around 2.5 quintillion bytes of data are generated every single day and its value just keeps increasing. But on the other hand the need to protect data has also up surged due to security requirements. In this paper we discuss about various watermarking techniques that have been developed at different domains for the same reason and compare them. We focus mainly on digital data such as images and how to preserve its authenticity as well as detect unauthorised tampering using watermarking techniques. At the later part of the paper i have proposed and implemented a basic watermarking technique and discussed the same.**

I. Introduction

Due to ease of access to internet connectivity to almost every houses, the data access, distribution / circulation has become easier and faster. Any person can download a data over internet and instantly share it with masses. So the need for protecting the authenticity of the data has increased in order to preserve its novelty and to make them tamper-evident rather than making it tamper-resistant. The simple difference both is that tamper-evident indicates that the data has been manipulated by an unauthorised entity rather than trying to prevent the tampering process as such which seems much more of a difficult task.

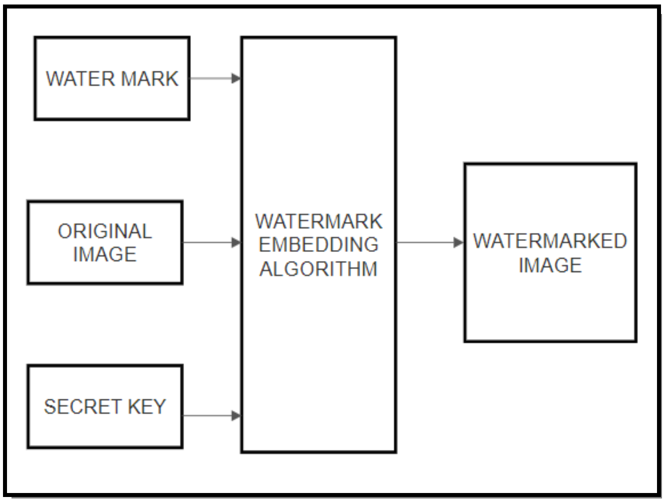
Watermarking is one of the widely used techniques with which a message / secret key / data is embedded along with the image and is transformed on a particular domain or a combination of domains. In most scenarios the watermarking is made invisible and can't be rendered through human eye. Specialised algorithms are required in order to extract the data from the digital media. The process of extraction can be done to cross verify the image signature to preserve its integrity.

Only the authorised entity has access to both the digital signature and the specialised algorithm to transform/extract the corresponding information, thus securing access control. The attacks on a particular image could either be deliberate such as morphing or cropping whereas sometimes they are inadvertent such as compression or Digital to Analog conversion Based on the degree of attack on the image they are broadly classified into three types:

1) Simple attacks are those in which the watermark of the image undergoes major changes. These are performed by those who don't care much about the changes done to the watermarks and therefore the attack is detectable. E.g. Cropping

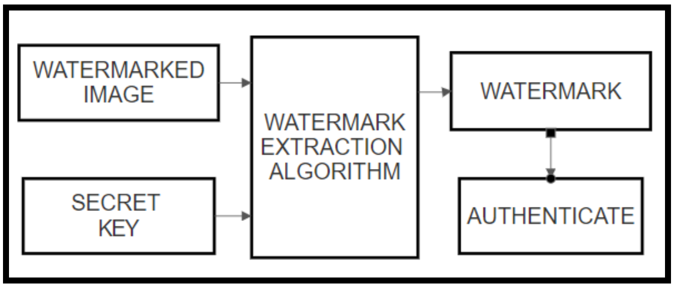
2) Second degree attacks are those in which the watermarks undergo slight modification. These attacks can be detected using statistical correlation and in most cases using specialised methods the original watermark may even be acquired back.
E.g. Geometric Distortion or Pixel Manipulation

3) Third degree attacks are those in which the validity of the watermark is removed. This could be done by either adding multiple watermarks on the same image thereby making the authoritative watermark hidden or by separating the watermark from the image and discarding the signature, so that the image distribution further cannot be traced back. These often come under the category of deliberate attacks.



PROCESS OF CREATION OF WATERMARKED IMAGE

The digital image along with a large prime number which acts as a secret key and a watermark is passed as inputs to the watermark embedding algorithm which generate a secured unique watermarked image.



PROCESS OF EXTRACTION OF WATERMARK

For the process of extraction of the watermark the watermarked image is combined with the user's secret key and passed as input to the inverse algorithm which then generates the required watermark. Further the obtained watermark is cross verified to detect attack(s).

Applications:

1) **Live Feedback**: This is one of the major uses of watermark with which a particular information for example number of people watching the live stream currently etc. can be sent secretly along with the image frames even to remote geographical locations where they can be decoded.
2) **Preserve Copy Right**: Due to easy replication of images in an instant the novelty of the original image along with its creator is lost. Watermarking can be implied here to solve this issue and preserve authenticity
3) **Piracy Protection:** piracy is one of the major problems that the whole film industry is facing, with the help of watermarks the DVD players or Video players can be programmed in such a way that only if the watermark is original then the content inside the media fie should be played
4) **Piracy Tracking**: Similar to the above scenario here for every user who has subscribed for a particular channel has access to videos being posted. When that person tries to share the video, the unique watermark corresponding to the user can be obtained and the user can be traced easily.
5) **Order Verification**: Sometimes instead of QR Codes Bar codes for object detection the watermarks can be used instead as they are harder to replicate and are heavy
6) **Block Adult Content**: The child safety plugin in web browser is a perfect example where the adult content images and videos can be watermarked uniquely and when the child tries to open such page the content can be automatically blocked or blurred. Similarly based on the interests and behaviours of the user's the contents can be prescribed accordingly

II. Literature Survey

MEETA MALONIA et.al put forward a digital water marking method that works on Discrete Wavelet Transform and Arithmetic Progression algorithm. He used arithmetic progression to enclose binary watermarks within a digital image. This resulted into a watermark generation technique that has high perceptibility and robustness.

MAREK CANDIK et.al proposed a 2 level discrete wavelet transform and for smaller image sixes a 3 level DWT is employed. Then they tested a watermarked grey image of Einstein and investigated the overall distortion. Their process includes a encoding part where they decompose images in frequency domain and a Boolean set which holds 0s and 1s is used that denotes whether to transform the corresponding factor or not.

NAWAF HAZIM et.al states that the discrete cosine transform performed independently and discrete wavelet transform performed independently give good results but their robust nature still falls low. He proposed a technique combining both and proved that his results had very high robust quality compared to spatial domain transforms.

UNMESH MANDAL et.al presented a novel method using DWT with which they disintegrated the image into multiple factors. Then using the factors they obtained appropriate pixels or a group of the pixels which can be considered for watermark embedding process. Then they tested their method using PSNR to calculate perceptual transparency property and also Accuracy of the extracted watermark was measured.

WEI DING et.al proposes various methods for watermarking by transforming the frequency coefficients. He also discussed the pros and cons of Pita's method and few others. He used a 3 dimensional discrete wavelet transform. His results show extremely robust watermarks.

SAMIR BANDHYOAHDHAY et.al came up with a new a solution to problem when users require visible watermark sometimes and invisible watermark sometimes. His algorithm takes digital image and a watermark to produce two watermarked image one visible and other invisible using DWT. He further says future work can be done on making the decomposition process on further levels to produce stronger mark.

Z.Z.WANG et.al. Solves the problem faced by most of the approaches where size of the watermark is larger than the original image. In his model the length of the watermark is proportional to the digital image. If the image is too large then the length was restrained to particular value. He used discrete cosine transform to encode and decode.

III. Watermarking techniques based on different domains

Discrete Fourier Transform:
In this transform the image is processed into a sum of sine and cosine functions of N discrete time samples into N discrete frequency samples. Used for Fourier analysis.

DFT for a sequence of complex no is defined as follows:

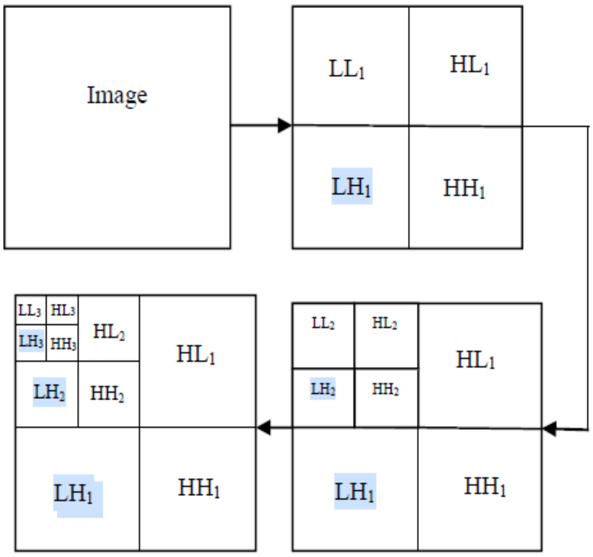
$$F(u,v) = \sum_{m=0}^{M-I}\sum_{n=0}^{N-1} f(m,n)e^{-j2\pi(\frac{km}{M}+\frac{nl}{N})}$$

Discrete Cosine Transform:
This is very much similar to DFT as it converts the signal in spatial domain to frequency domain but in terms of sum of elementary cosine functions. This is widely used for image compression and pattern recognition. Here watermarking is based on non-overlapping blocks which results into three further sub bands low, mid and high frequency. DCT watermarking is based on two main things, firstly the significant details about the image lies in lower frequency bands and the rest of information at higher frequency bands maybe lost during compression or image processing.

General equation of a DCT signal is as follows:

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

Discrete Wavelet Transform:
Wavelets are discretely sampled here. Applying a DWT is similar to passing the signal into filters that segregates or decomposes the signal into four main sub-components namely LL1, LH1, HH1, HL1.Then each sub-component is again decomposed into further components.



LL- The low frequency sub-band of the digital image which contains the approximation of the image.
HL1- This constitutes Horizontal details of the image.
LH1- This constitutes Vertical details of the image.
HH1- Constitutes the High Frequency details image.

Singular Value Decomposition:
“Singular value decomposition (SVD) is
a factorization of a real or complex matrix that
generalizes the Eigen decomposition of a
square normal matrix to matrix via an extension of
the polar decomposition.”

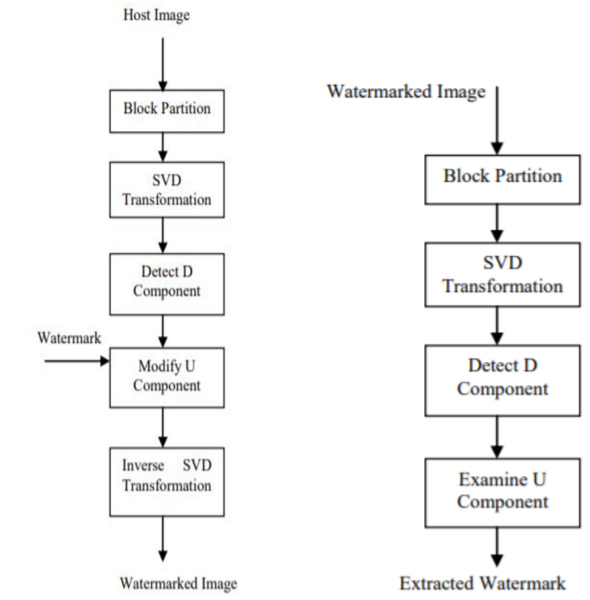
A digital Image X of size MxN, with M≥N, can be represented by its SVD as follows;

$$\overset{N}{[X]}_{M} = {}_{M}\overset{M}{[U]}\ \overset{N}{[S]}_{M}\ \overset{N}{[V]}^{T}{}_{N}$$

$$U= [u_1, u_2, \ldots.\ u_m], \qquad V=[v_1, v_2, \ldots.\ v_n]\ ,$$

$$S = \begin{bmatrix} \sigma_1 & & & \\ & \sigma_2 & & \\ & & O & \\ & & & \sigma_n \end{bmatrix}$$

SVD is an effective tool to analyse the matrices. In this technique the matrix is decomposed into three sub matrix namely X, D and Z.
U, Z- are the unitary matrix
V-Diagonal matrix



Encoding and Extraction of Watermark in SVD

IV. Comparative Study

The following table presents a comparative study between DCT, DWT and DFT in terms of watermarking based on study.

Method	Advantage	Disadvantage
Discrete Fourier Transform	1)Rotational resistant 2)Translation Invariant 3) High robustness 4) Performs best under geometrical attacks	1)Due to approximation through the process the accumulation of error increases. 2)Loss of quality while extraction process 3)Time taken is also much higher
Discrete Cosine Transform	1) Since the image is decomposed into multiple levels here the middle frequency level can be used to embed the required watermark which makes it more resistant towards attacks that affect the low or high frequency 2)Compared to spatial transforms this is more robust in nature	1) Loss in quality of image when compressed
Discrete Wavelet Transform	1) Spatio-frequency localisation is better. 2) Increased Versatility. 3) High imperceptibility. 4)Can carry more watermark with decent concealing effect	1) Adding watermark might degrade image. 2) Implementation cost is very high
Singular Value Decom-position	1) Produces least mean square truncation error. 2) Deals in matrix level. 3) Highly Stable. 4)Uses variable orthogonal basis hence the error is very low	1) Sensitive to noise in general 2) Low Distortion is experienced here

Thus every transform technique has its own unique advantage as well as some disadvantage in different standards. Hence the ideal algorithm that can be used for a variety of purpose would be combination of all the above mentioned as certain characteristics from certain technique would give us an ideal result.

V. Experiment

The objective of this section is to understand how different domains techniques work and how they are respond towards a particular attack.

The host image throughout this experiment would be:

The secret watermark that will be embedded would be:

Packages Used:

- Numpy - Numeric Python
- CV2 - Open-CV
- PYWT - PyWavelets

1) Discrete Fourier Transform:

Code:

```
def DFT(coverImage, watermarkImage):
    coverImage = cv2.resize(coverImage, 
(300, 300))
    cv2.imshow('Cover’, coverImage)
    watermarkImage = 
cv2.resize(watermarkImage, (300, 300))
    cv2.imshow('Watermark Image', 
watermarkImage)
    watermarkedImage = 
applyWatermarkDFT(coverImage, 
watermarkImage, 10)
    watermarkedImage = 
np.uint8(watermarkedImage)
    cv2.imshow('Watermarked Image', 
watermarkedImg)
```

2) Discrete Cosine Transform:

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

3) Discrete Wavelet Transform:

Code:

```
def DWT(coverImage, watermarkImage):
    coverImage = cv2.resize(coverImage,
(300, 300))
    cv2.imshow('Cover Image',
coverImage)
    watermarkImage =
cv2.resize(watermarkImage, (150,   150))
    cv2.imshow('Watermark Image',
watermarkImage)
    # DWT on cover image
    coverImage = np.float32(coverImage)
    coverImage /= 255;
    coeffC = pywt.dwt2(coverImage,
'haar')
    cA, (cH, cV, cD) = coeffC
    watermarkImage =
np.float32(watermarkImage)
    watermarkImage /= 255;
    # Embedding
    coeffW = (0.4 * cA + 0.1 *
watermarkImage, (cH, cV, cD))
    watermarkedImage =
pywt.idwt2(coeffW, 'haar')
    cv2.imshow('Watermarked Image',
watermarkedImage)
```

3) Singular Value Decomposition:

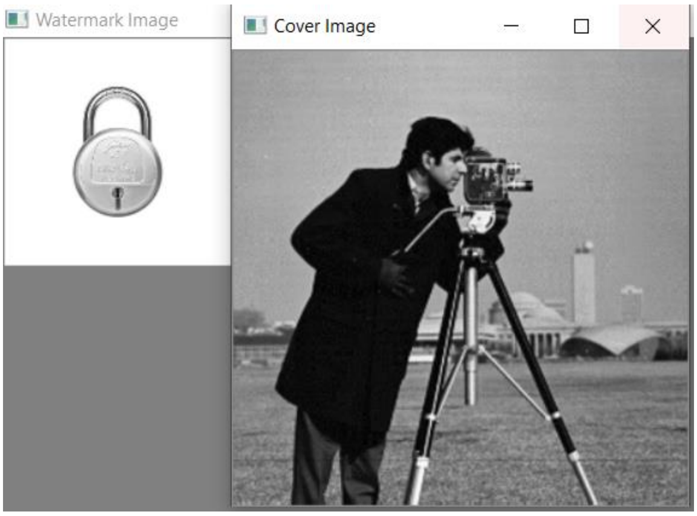
Code:

```
def SVD(coverImage, watermarkImage):
    [m, n] = np.shape(coverImage)
    coverImage = np.double(coverImage)
    watermarkImage =
np.double(watermarkImage)
    ucvr, wcvr, vtcvr =
np.linalg.svd(coverImage,
full_matrices=1, compute_uv=1)
    Wcvr = np.zeros((m, n), np.uint8)
    Wcvr[:m, :n] = np.diag(wcvr)
    Wcvr = np.double(Wcvr)
    [x, y] = np.shape(watermarkImage)
    # modifying diagonal component
```

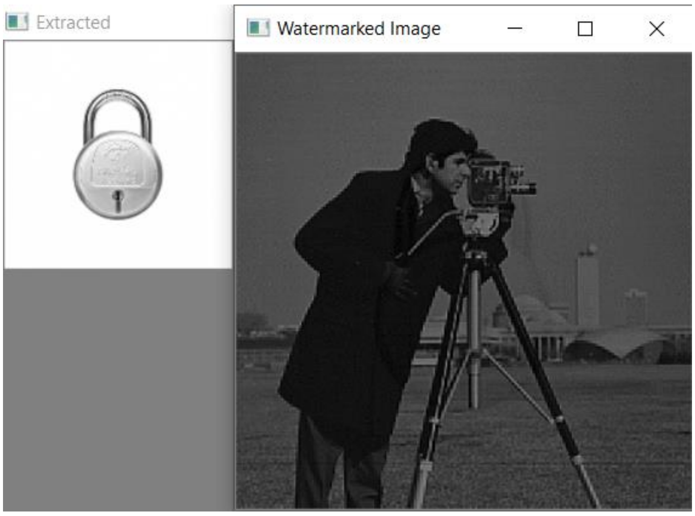
```
 for i in range(0, x):
        for j in range(0, y):
            Wcvr[i, j] = (Wcvr[i, j] +
0.01 * watermarkImage[i, j]) / 255

    # SVD of wcvr
    u, w, v = np.linalg.svd(Wcvr,
full_matrices=1, compute_uv=1)
    # Watermarked Image
    S = np.zeros((225, 225), np.uint8)
    S[:m, :n] = np.diag(w)
    S = np.double(S)
    wimg = np.matmul(ucvr, np.matmul(S,
vtcvr))
    wimg = np.double(wimg)
    wimg *= 255
    watermarkedImage =
np.zeros(wimg.shape, np.double)
    normalized = cv2.normalize(wimg,
watermarkedImage, 1.0, 0.0,
cv2.NORM_MINMAX)
    cv2.imshow('Watermarked Image',
watermarkedImage)
```

Cover Image + Watermark



Extracted Watermark + Watermarked Image



Variations in watermarked image:

a) Zoom

b) RGB mix 1

c) RGB mix 2

d) Invert

e) Blur

To calculate error we use MSE(Means Square Error) Between the original watermark and the extracted watermark after attack

```
def mse(imageA, imageB):
    err = np.sum((imageA.astype("float")
- imageB.astype("float")) ** 2)
    err /= float(imageA.shape[0] *
imageA.shape[1])
    return err
```

VI. Result

Attack	DCT_DWT_SVD
ZOOM	45021 MSE
RCB MIX 1	60293 MSE
RGB MIX 2	41873 MSE
INVERT	26410 MSE
BLUR	69700 MSE

Better results are shown at an average for all types of attacks when it comes to DCT_DWT_SVD combination This implementation is much robust and versatile.

VII. Conclusion

Digital Watermarking is one of the growing applications which can be used for a variety of purposes as discussed above. A good transform technique is the one that is capable of performing well under most conditions and against most attacks. The watermark embedding process shouldn't be a very complex, which uses high cost and computational time. Also the produced watermark image should be very much similar to the original host image to ensure that the watermark is immersed thoroughly.

The extraction process should also be efficient and the extracted watermark should be utmost similar to the implanted watermark. We have discussed in detail about SVD, DFT, DWT, DCT and DCT_DWT_SVD and tested them against ZOOM, RCB MIX 1, RGB MIX 2 INVERT, BLUR. The combined technique DCT_DWT_SVD showed better results and proved robust.

The future work can be done on including multiple watermarks into same image to make them more efficient. Also the tests can be performed for different types of image formats (we have used jpeg here) like PNG, BMP.

VII. References

[1] Malonia, M., & Agarwal, S. K. (2016, March). Digital image watermarking using discrete wavelet transform and arithmetic progression technique. In 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (pp. 1-6). IEEE.

[2] Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. (pp. 709-716). IEEE.

[3] Tyagi, S., Singh, H. V., Agarwal, R., & Gangwar, S. K. (2016, March). Digital watermarking techniques for security applications. In 2016 International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES) (pp. 379-382). IEEE.

[4] ČANDÍK, M., MATÚŠ, E., & LEVICKÝ, D. (2001). Digital watermarking in wavelet transform domain. Radioengineering, 10(2), 1-4.

[5] Jayashree, N., & Bhuvaneswaran, R. S. (2019). A robust image watermarking scheme using z-transform, discrete wavelet transform and bidiagonal singular value decomposition. Computers, Materials & Continua, 58(1), 263-285.

[6] Singh, S. P., Rawat, P., & Agrawal, S. (2012). A robust watermarking approach using DCT-DWT. International journal of emerging technology and advanced engineering, 2(8), 300-305.

[7] Sharma, G., Chawla, R., Gupta, S., & Dora, S. (2019). A publicly verifiable watermarking scheme based on quantum chaos and DWT–DCT. SN Applied Sciences, 1(12), 1699.

[8] Abdulrahman, A. K., & Ozturk, S. (2019). A novel hybrid DCT and DWT based robust watermarking algorithm for color images. Multimedia Tools and Applications, 78(12), 17027-17049.

[9] Xi, X., Zhang, X., Sun, Y., Jiang, X., & Xin, Q. (2020). Topology-Preserving and Geometric Feature-Correction Watermarking of Vector Maps. IEEE Access, 8, 33428-33441.

Others:

1)https://en.wikipedia.org/wiki/Discrete_cosine_transform

2)https://users.cs.cf.ac.uk/Dave.Marshall/Multimedia/node231.html

3)http://en.wikipedia.org/wiki/Discrete_Fourier_transform

4)http://home.engineering.iastate.edu/~julied/classes/ee524/LectureNotes/l5.pdf

5) https://github.com/yingqichao/Robust-Digital-Watermarking-for-Color-Images-in-Combined-DFT-and-DT-CWT-Domains

6) https://github.com/Call1st0/dft-based-watermarking-method-with-GCR-masking