

# Securing Multimedia Content Using Watermark and Digital Signature

**Abstract**— Digital signature and watermarking are the processes combined together to guarantee the authentication and privacy of the data as well as copyright claims. With the increasing rate of multimedia usage, many processes have been introduced to ensure the safety of the contents. Over the years, these technologies have been able to secure the data safety of text documents but securing multimedia contents have been a very hard task to do. So, here using the data signature and watermarking along with cryptography, the multimedia data will be embedded with another data through watermark embedding and will be transmitted by after encrypting it using the cryptography algorithm. The receiver end on the other side will decrypt the data and extract the real data from the watermark. For digital watermarking, various transformation have been suggested. Among them the Discrete Wavelet Transformation (DWT) have shown the most accurate results. We will be using DWT for watermarking. And Inverse4 Discrete Wavelet Transformation (IDWT) will be applied at the time of extracting the real image.

**Keywords**— *Digital signature, Watermarking, Cryptography, DWT, IDWT, Watermark embedding, Multimedia content*

## I. INITIATION

With the instantaneous progress in the field of data science, software and multimedia, securing personal data and contents is becoming harder day by day [1-2]. Duplication and unauthorized usage of multimedia has increased by far [3]. With these increasing usage of data, new security systems and softwares are also getting introduced [4]. In this research implementation of security system by applying the method and operation known as digital signature and watermarking will be introduced and explained [5-6]. Digital signature is such a set of features that is created in an automated way and gets encrypted and stored in a file or content and gets decrypted accordingly by some encryption and decryption algorithm which are produced by using the method of cryptography [7-8]. Digital signature is similar to a paper signature that is put on a digital content such as image, digital document and other files. Watermarking is a process where data or information is embedded into a digital signal or media which will signify the uniqueness, copyright and authenticity of the digital signal [9]. Applied watermarking is implemented properly and it will be very difficult to erase. These techniques will follow the cryptography algorithm. So far, the approached and applied methods to secure data has been satisfactory [10].

The researchers are taking challenges a step ahead for better outcomes, making the watermarking process more enriched and secure. In the past few years, image and video watermarking have become the key research for the researchers [11-14]. But the video watermarking process is

implemented in the same way as image watermarking which is directly applied to the real video to compressed video which makes the video data less secure and easier to plagiarize [15-16]. Thus these processes are yet not secure enough to confirm user privacy and authentication. So, the prime objective of our research is to transmit the digital data to the receiver with maximum security and extract the watermark back to its initial form.

## II. LITERATURE VIEW

In [17], a brief discussion on various image watermarking is found. There processes included spatial and frequency transfer domain and their sub-domains namely LSB technique, SSM modulation based techniques, Discrete Cosine Transformation, Discrete Wavelet transformation and many more. The paper also gives a detailed idea of these processes and their effectiveness. In [18], the embedding of watermarking and digital signature in an image and how it can resist Holliman Memon attack is described. This process can save image data from tempering and recover the real data.

M. S. Murty et al. [7] explains the process of image authentication using watermarking and digital signature. Before sending the image, it is first watermarked for authentication and after that digital signature is applied for encrypting the data properly. After receiving the image data, decryption is applied and the real data is received by the receiver. M. Ahmed et al. [19] applied chaotic theory. The encryption and decryption of image data is accomplished by chaotic mapping and cryptography algorithm.

Another paper by Dr. V. Suma [20] depicts the distributed cloud information retrieval by using deep fuzzy hashing algorithm. In this method, hashing efficiently retrieves the information based on mapping the same data as correlated binary codes and this data is trained using deep neural network and fuzzy logic. This method shows more efficiency than the conventional methods. By applying this method the data management in cloud computing can be modified.

At first the digital signature is applied on the real image through RSA encryption algorithm. This digital signature then watermarked and transmitted to the receiver and decrypted into real image. The digital signature is extracted in the process of decryption. But slight changes in image such as compression, filtering will make the digital signature impair its robustness. To avert this vulnerability, watermarking process can be applied and it can protect the integrity of the content even after the fluctuation of the

image. So we will be embedding these two and encrypt the real data before transmission.

### III. RESEARCH METHODOLOGY

On the basis of domain, watermarking can be classified into two domains. They are spatial domain watermarking and frequency domain watermarking. The spatial domain approach is established by updating the pixels. The spatial transform system is also divided into two types: SSM modulation based technique and Least Significant Bit (LSB) technique. LSB is usually applied in case of spatial Domain.

On the contrary, Frequency Domain Approach works on the frequency representation of the image. This approach is more efficient than the spatial domain approach and the outcomes are also more accurate. In this process the image is first sliced into frequency bands and watermark is embedded to it. Thus it is converted into watermarked image. The inverse conversion is applied for the watermarked image. Frequency domain technique is classified into two sub domain types: Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT). In DCT the frequency is divided into many frequency bands. And in DWT the image is broken down into many orders or sublevels and classified as small frequency wavelets.

Following some procedures sequentially, watermarking will be done. DWT, RSA encryption, IDWT, image embedding, decryption and watermark extraction process will be done throughout the process.

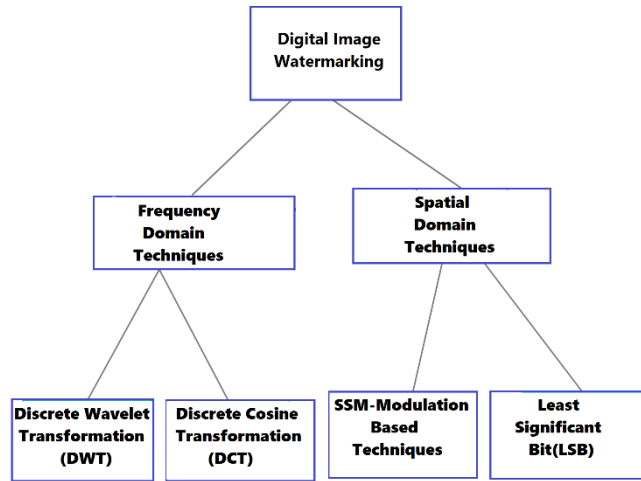


Fig. 1: Digital Image Watermarking Classification.

In our proposed scheme, the real image is first divided into sub-bands by applying DWT and has been decomposed into a frequency domain. On the other hand, the watermark has been encrypted by RSA encryption and has been embedded with the decomposed real image data. After reaching at the receiver's end IDWT is applied and the decomposed image data has been upscaled. After that, the watermark is extracted and the data is decrypted. Thus, the real image data is returned.

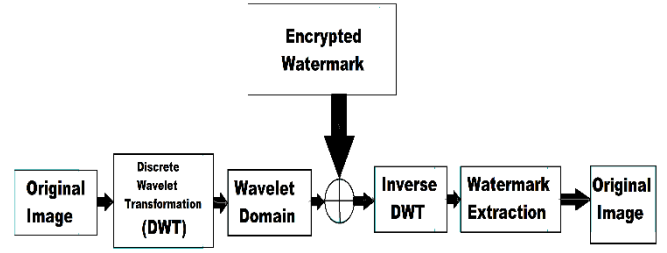


Fig. 2: Block diagram of methodology.

#### A. Discrete Wavelet Transform (DWT) technique

We will be operating through DWT for our watermarking. DWT creates both spatial and frequency domain of the image. In this transformation the temporal data is preserved. A fixed function is used to organize the wavelets which is known as mother wavelet. The mother wavelet creates small sub-bands of wavelets of the 2-D image. In this decomposition, the 2-D image is processed and filtered into four sub-bands.  $LL$ ,  $HL$ ,  $LH$ ,  $HH$ . Here  $LL$  is the low frequency part which represents the coarse scale DWT coefficient which can again be decomposed into another 4 sub-bands. The  $LL$  sub-band visualizes the approximation of the image data. On the other hand the  $HL$ ,  $LH$ ,  $HH$  are horizontal high frequency part, vertical high frequency part and high frequency part. These sub-bands are fine scale DWT coefficients. These parts contain very high frequency resolutions and cannot be scaled further. These sub-bands show the specific data of the image. Thus by scaling, the real image frequency can be divided into many sub-bands depending on the slicing. If there is ' $n$ ' number scaling, then there will be  $(3n+1)$  numbers of sub-bands of that real image. Thus it will create a big amount of sub-bands containing varieties of frequency bands which will make the specification in embedding more accurate and simple. The sub-band here will start from 1 till  $LLn$ . Thus by this process we can scale the low frequency portion into lower bands. Depending on the scaling the decomposition is classified. If the decomposition is done once, it's called first level decomposition. If it's done twice, it's called 2<sup>nd</sup> level decomposition and so on. In our implementation we will be working mainly on the 1<sup>st</sup> level decomposition. Also experimental results will be shown on 2<sup>nd</sup> level DWT. After completing the DWT the watermark will be embedded which will be robust. This process is quite easy to implement and the result is also much sophisticated.

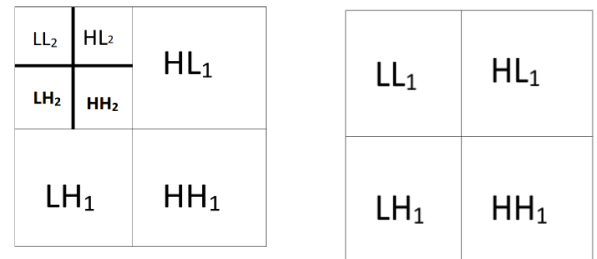


Fig. 3: 1<sup>st</sup> and 2<sup>nd</sup> level DWT.

To apply DWT on a signal, necessary equations have to be followed. Suppose an image signal  $A$  is needed to be scaled through DWT. First the data of  $A$  is passed through a low pass filter  $f$  with an impulse response. Convolution occurs between the image signal  $A$  and the impulse signal. The output from this low pass filter gives the approximation co-efficient which is of low frequency. The image signal is

also passed through a high pass filter  $g$ . The high frequency sub-bands is passed through this filter  $g$ . The output of this high pass filter gives detail coefficients of the image data  $A$ . These two filters are known a quadrature mirror filter. Following the Nyquist's rule, the main frequency band is divided into two. The low frequency band is again passed through the high-pass and low-pass filters  $f$  and  $g$  making the cut-off frequency half of the previous one. By this process the low frequency achieved before is sub-scaled into two more frequencies following the same process again. In the decomposition, as the time resolution is halved, the frequency resolution has been doubled. For the convolution, the equation is:

$$Y[n] = (A * f)[n] = \sum_{h=-\infty}^{\infty} A[h] f[n-h] \quad (1)$$

Following the convolution equation,

Equation for low-pass filter:

$$Y_{LOW}[n] = \sum_{h=-\infty}^{\infty} A[h] f[2n-h] \quad (2)$$

Equation for high-pass filter:

$$Y_{HIGH}[n] = \sum_{h=-\infty}^{\infty} A[h] g[2n-h] \quad (3)$$

As the frequency resolution is doubled,  $2n$  is used instead of  $n$ .

Using subsampling operator,  $(Y \downarrow h)[n] = Y[h n]$

(2) and (3) can also be written like:

$$Y_l = (A * f) \downarrow 2 \quad [\text{For low-pass-filter}] \quad (4)$$

$$Y_h = (A * g) \downarrow 2 \quad [\text{For high-pass filter}]$$

Now, the equation for the decomposition of the matrix form:

$$R = \quad (5)$$

$XYZ^T$

Here,

$X = p \times p$  matrix

$Z = q \times q$  matrix

$Y = p \times q$  diagonal matrix

$Z^T$  = Transformation matrix of  $Z$

$R = p \times q$  matrix of the real image

## B. RSA Cryptography

Cryptography is an input based algorithm which performs both encryption and decryption of data from sender to receiver ensuring the integrity of the data. The encryption and decryption is established using key. There can be two types of keys: public key and private key. Depending on these keys there are two major cryptography. They are symmetric and asymmetric cryptography. In symmetric cryptography both sender and receiver will obtain the same key. On the other hand in asymmetric cryptography both public and private keys will be applied. Sender will apply one key for encryption. The receiver will receive the data known as ciphertext and use the other key to decrypt to get the real data. Depending on these two there are several algorithm such as Caesar's method or shift cipher method, Block Cypher method, RSA cryptosystem, DSA cryptosystem etc. The symmetric cryptography is less secure as only one key is use in these kinds of cryptography. For which the data may get sabotaged. The asymmetric cryptography in that case is the most acceptable option.

Here we will be using RSA cryptography algorithm. This is a public key or asymmetric cryptography system. The name RSA came from the surname of three inventors Ron Rivest, Adi Shamir, and Leonard Adleman. In this cryptosystem, the sender will input two random prime numbers based on which the algorithm will generate public and private keys. Using the public key data will be encrypted and will be sent to the receiver. The encoded data is known as ciphertext. The receiver will decrypt the ciphertext using private key and get the data. The main advantage of this system is, the keys are generated and even if any third party gets the public key, the data won't get harmed in the process as private key works as a decryption key in this process. As block cipher and shift cipher are both symmetric cryptosystems, these are less efficient and less secure. Besides that, any third party can even apply all the possibilities in the shift cipher method as there are only 26 for each text. But the RSA cryptosystem uses two keys for both encryption and decryption. Minimum key size for RSA is 512 bits for public key dataset and 1024 bits for token key data set which makes impossible for the third party to predict the key and sabotage the system.

The DSA is an asymmetric cryptographic system like RSA cryptosystem. Both cryptosystems contain almost the same strength and the key size are also same for both cryptography system. RSA cryptography relies on prime factorization, while DSA uses the discrete logarithm problem. But RSA performs better in terms of encryption and verification. DSA works better in decryption and signing. So, for RSA is considered proper for our implementation.

*Equation and procedure:*

Let's say two input prime numbers are  $X$  &  $Y$ .

Step-1: For public key member,  $a = X*Y$

Step-2:  $F(a) = (X-1)*(Y-1)$

Here,  $F(a)$  is the Euler's totient function

Step-3: For another member for public key, let's take an integer  $m$  such that,

$$1 < m < F(a)$$

And  $\gcd(m, F(a)) = 1$ ; which means  $m$  and  $F(a)$  has to be co-primes.

Step-4: For private key let's take  $d$  such that,

$$m*d \equiv 1 \pmod{F(a)}; \text{ where } 0 \leq d \leq a$$

Step-5: public key =  $(m, a)$

Private key =  $(d, a)$

Step-6: For encryption-

$$\text{Encrypted data} = (\text{Real data})^m \pmod{a}$$

For decryption-

$$\text{Real data} = (\text{Encrypted data})^d \pmod{a}$$

Here, a block can be defined by one or more digits having one letter or data where each smallest unit of data will be expressed by two digits. It should be noted that, the value for each block must not exceed the value of  $a$ .

### C. Watermark Embedding

The watermark image at first was manipulated in such way that it was not understandable visually. In this process, pixels with their nearest pixels correlate with each other creating a distortion like image which may seem broken. But the pixels maintain their values, which ensures their authenticity. The pixelated image was encrypted afterwards. At this point the watermark image is reconstructed and embedded with the reshaped host image which was previously done through DWT. The watermark image is reformed into a one dimensional array. Let's say the pixel values of the watermark image has  $p$  number of rows and columns, creating a  $p \times p$  matrix. This matrix is restructured into a  $1 \times (p \times p)$  or  $1 \times p^2$  matrix which can be defined as  $F$ . The columns from the  $p \times p$  matrix were taken serially to form the array. The array has  $p^2$  number of values. An array is also represented by  $b(i)$  where  $i$  ranges from 1 to  $p^2$ . The initial value  $b(0)$  and another parameter  $n$  has to be inputted where,  $0 < b(0) < 1$  and  $3.5699456 < n < 4$ . Following the inputs, the array gets reconstructed by a order in range of  $(0, 255)$ . The values for  $a(i)$  will be regenerated by the given formula below,

$$b(i) = \text{mod}(\text{round}(x*(y*b(i) - \text{round}(y*b(i)))), 256),$$

$$\text{round}(y*b(i)) < y*b(i)$$

$$\text{and } b(i) = \text{mod}(\text{round}(x*(1-y*b(i) - \text{round}(y*b(i)))), 256),$$

$$\text{round}(y*b(i)) > y*b(i)$$

$00x$  and  $y$  here are defined as amplification factors. The round function rounds up the float value to its nearest integer value. The array and new one dimensional matrix is operated through a exclusive X-OR gate.

$$F'(i) = \text{bitxor}(b(i), F(i))$$

$F'(i)$  is the new form of  $F(i)$  which is manipulated pixel wise. Maintaining the order of  $F$ ,  $F'$  is also a  $1 \times p^2$  matrix.  $F'$  matrix is again reshaped to form the previously ordered  $p \times p$  which is the encrypted watermark image. For further security, the inputted values of  $b(0)$  and  $n$  is encrypted through *RSA cryptography* algorithm using a public key and turned into ciphertexts. After encryption the encrypted watermark image is inserted into the host image and the watermarked image is formed. The watermarked image is transmitted to receiver side and the ciphertext is decrypted using private key. Described steps for the insertion of watermark image is given below,

1. Following the *RSA cryptography* algorithm described previously, the values of  $b(0)$  and  $n$  is encrypted using the public key.

2. Using the parameters of  $n$ , the grayscale watermark  $M$  is reshaped to a rearranged unreadable pixelated form  $M'$ .

3. Using DWT, the grayscale host image  $H$  is decomposed into four sub-bands LL, HL, LH, HH.

4. Equation for decomposition was applied on the lowest frequency band LL.

$$R_{LL} = X_H, Y_H, Z_H$$

5. Reformed the singular value to  $Y_H'$  by adding  $Y_H$  with the reshaped watermark  $M'$  multiplied to a scaling factor  $\beta$ ,

$$Y_H' = Y_H + \beta \cdot M'$$

6. Decomposition equation applied on the new singular value  $Y_H'$ ,

$$R_{LL}(Y_H') = X_M, Y_M, Z_M$$

7. To replace the low-frequency approximate co-efficient a  $LL_{\text{new}}$  is formed using decomposition equation,

$$R(LL_{\text{new}}) = X_H, Y_M, Z_H'$$

8. The watermarked image  $H_M$  is formed using Inverse DWT (IDWT) using  $LL_{\text{new}}$ .

### D. Inverse Discrete Wavelet Transformation (IDWT)

The IDWT can be introduced as the opposite process of DWT. The IDWT combines all the sub-bands which was decomposed in DWT. The scaled approximation and detail frequency coefficients will go through upsampling. Upsampling is a process where the frequency coefficients will be separated or sampled by inserting zero valued samples in between the frequency sub-bands. Through the process of upsampling, the length of the coefficients get doubled. After that the sub-bands of approximation and detail coefficients are combined separately using the reconstruction filters following the convolution equation. As the two coefficients are reconstructed, they are assembled together to get the real image back. Here the approximation coefficients are combined using scaling filter and detail coefficient is combined by wavelet filters.

Let's take  $n$  as the length of the scaling filter. So, the first  $(n/2 - 1)$  number of coefficients have to be taken and add at the end to make them periodic. The unnecessary part of the convolution is needed to be removed. For this the coefficients from  $n$  to  $n-1$  has to be taken. Thus we will get our real image.

#### E. Watermark extraction

After obtaining the new singular value  $Y_H'$  and the modified host image watermark extraction is executed following the steps below:

1. The host image  $H$  and the watermarked image  $H_M$  gets decomposed into four sub-bands in 1<sup>st</sup> level DWT where  $H$  gets decomposed into  $LL$ ,  $HL$ ,  $LH$ ,  $HH$  and  $H_M$  gets decomposed into  $LL_M$ ,  $HL_M$ ,  $LH_M$ ,  $HH_M$ .

2. Decomposition formula is then applied on  $LL_M$  following the equation below:

$$R(LL_W) = X_{HM} \cdot Y_{HM} \cdot Z_{HM}$$

3. Low-frequency approximate coefficient is updated at this point. Here,

$$LL_{new}' = X_M \cdot Y_{HM} \cdot Z_M'$$

4. Watermark image is reformed by the given formula:

$$M'_{new} = (LL_{new}' - Y_H) / \beta$$

5. The cypher text at this point is decrypted using the private key following the RSA Cryptography algorithm. Thus the real data  $b(0)$  and parameter  $n$  is retrieved.

6. With the parameter  $n$  the watermark image is retrieved to its original form.  $b(0)$  is also applied here.

#### IV. EXPECTED OUTCOME

Software used for the implementation is python. The code is executed properly in versions equal to or above python 3.6. For additional module, NumPy, OpenCV and PyWavelets are installed. After running the code, digital watermarking process first takes the initial value  $b(0)$  and the parameter  $n$  in between the given range as input. It also takes the host image and watermark image path. After that, the process requires two prime key values to generate the public and private keys for encryption and decryption. The public key and private key that the algorithm provides have no interconnection with the given input by the user, thus ensuring the data security and privacy. Applying the public key values, data gets encrypted and the encrypted data is formed. The host image has been embedded with the watermark data and gets transmitted. On the receiver end, data gets decrypted by applying private key and the host image is extracted safely from the watermark image. The resolution of the real image persists the same quality as before after decryption.

Here, the two images have been selected as host image and watermark image accordingly for watermarking. The watermark image is 256×256 grayscale image and the host image is 512×512 grayscale image. After finishing the process, the watermarked image is obtained successfully which is of 512×512 resolution.



Host Image

Watermark Image



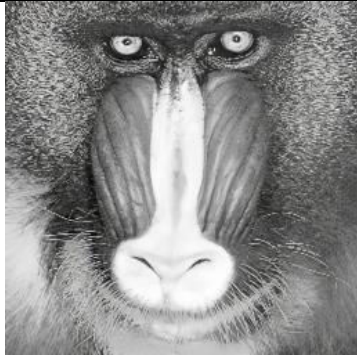
Watermarked Image

Fig. 4: Embedding watermark image into host image.

#### A. Tables

After generating the watermarking process, different values on different inputs have been obtained. Some of the experimental results are given below:

TABLE I. WATERMARK IMAGE VS. EXECUTION TIME

Watermark Image	Execution time (seconds)
 <p>256×256</p>	0.5564043521881104



 256x256	0.501476526260376
 256x256	0.5077581405639648
 256x256	0.5066986083984375

For RSA cryptography different values of prime numbers have been applied for watermarking using the watermark image that required least execution time for watermarking.

TABLE II. RETRIVAL TIME AT DIFFERENT RSA PARAMETERS



P r i m e  n u m b e r s	P u b l i c  k e y	P r i v a t e  k e y	P i c t u r e  r e t r i e v a
--	---	--	---


			l t i m e  ( s e c o n d s )
( ( 2 3 3 ,  2 8 1 )	( 2 5 4 6 1 ,  6 5 4 7 3 )	( 4 0 5 4 1 ,  6 5 4 7 3 )	0 . 5 2 3 6 1 7 0 2 9 1 9 0 0 6 3 5
( 1 0 7 ,  1 1 3 )	( 3 4 6 1 ,  1 2 0 9 1 )	( 8 0 1 3 ,  1 2 0 9 1 )	0 . 5 0 9 3 6 4 6 0 4 9 4 9 9 5 1 2
( 7 ,  1 3 )	( 1 ,  9 1 )	( 1 ,  9 1 )	0 . 5 0 1 4 7 6 5 2 6 2 6 0 3 7 6
( 1 3 1 ,  1 9	( 1 2 8 3 ,  1 ,	( 1 3 7 3 ,  ,	0 . 5 0 6 7 6 7 3 3

1	2	2	4
)	5	5	1
	0	0	7
	2	2	5
	1	1	1
	)	)	0
			9
			8
			6
			3
			0
	(	(	5
	2	3	0
(	4	1	4
1	6	2	8
7	1	9	6
3	5	5	4
,	,	,	6
			9
2	3	3	2
2	9	9	6
7	2	2	8
)	7	7	7
	1	1	9
	)	)	8
			8
			3

Accuracy of the unscrambled watermark with respect to original image has also been measured. Percentage of accuracy of the unscrambled watermark shown below:

TABLE III. ACCURACY PERCENTAGE

Watermark	Percentage of accuracy
	94.46738597211006 %
	95.62060160703089 %

	91.5745511581235 %
--	--------------------

### B. Performance Comparison

A comparative representation has been observed between the result of our proposed method and the method proposed by Al-Haj, Ali [21], which represents the combined implementation of DCT-DWT for digital image watermarking. Same host image of 512×512 resolution has been applied on both algorithms and the watermark images were inserted accordingly on both algorithms. The execution time on various images of 256×256 resolution through both algorithms have been observed.

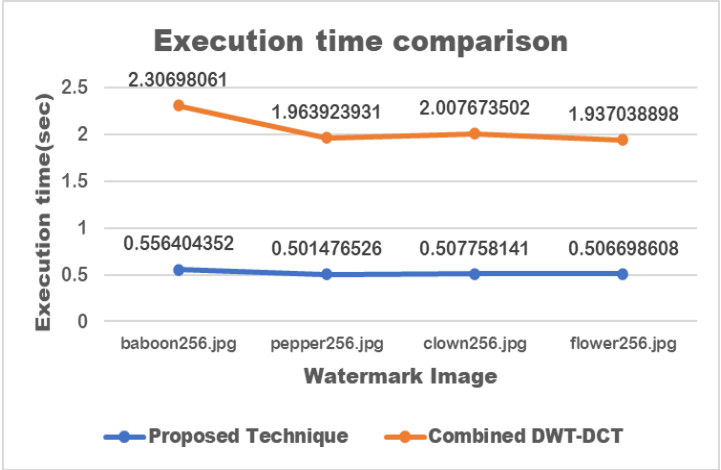


Fig. 5: Execution time comparison

From the graph, it can be said that, the execution time for our proposed method takes less time than the combined DWT-DCT method.

### V. CONCLUSION

The primary purpose of this paper is to create a robust watermarking system which can give a better outcome. The proposed watermarking process here is DWT which is more efficient compared to the other watermarking process as it can scale the frequency domains into many sectors. The process is easy and user friendly and the output gives strong protection to the data.

During the execution of the algorithm, it is observed that, for some small prime values as input for the encryption, the public and private keys are not produced properly. So, it should be kept in note that, large prime inputs for encryption

will give stronger and proper keys. Besides, in time of embedding, the initial value  $b(0)$  for the array  $b(i)$  is required to be kept between 0 and 1. Also for the parameter  $n$ , the value should be inputted in between 3.5699456 and 4. Otherwise, the embedding process shows error while execution.

By inputting high prime values, RSA cryptography gives more security to the data. Besides, after implementing IDWT and watermark extraction, original image data is extracted having the same pixels and resolution as before. The public and private keys used in the encryption and decryption process is also safe as private key cannot be obtained by any third party and without the private key, the original data cannot be extracted. The highest accuracy measured from the result is 95.62060160703089% which is also promising. The experimental outcomes also show that, the watermarking process takes less time, the efficiency is more than other processes and can ensure better security of the data. So, the multimedia data can be watermarked and digital signature can be applied more efficiently and in a faster way through this proposed method.

## VI. REFERENCES

- [1] Piva, F. Bartolini, and M. Barni, "Managing copyright in open network," *IEEE Transactions on Internet Computing*, vol. 6, no. 3, pp. 18-26, May-June 2002.
- [2] C. Lu, H. Yuan, and M. Liao, "Multipurpose Watermarking for Image Authentication and Protection," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1579-1592, October 2001.
- [3] C. Lu, S. Huang, C. Sze, and H. Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Transactions on Multimedia*, vol. 2, no. 4, pp. 209-224, December 2000.
- [4] J. Lee and S. Jung, "A survey of watermarking techniques applied to multimedia," In *Proc. of IEEE International Symposium on Industrial Electronics (ISIE 2001)*, vol. 1, pp. 272-277, Pusan, Korea, June 2001.
- [5] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593-1601, October 2001.
- [6] C.S. Lu and H.Y. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1579-1592, October 2001.
- [7] M. S. Murty, D. Veeraiah and A. Srinivas Rao, "Digital Signature and Watermark Methods for Image Authentication using Cryptography Analysis," *Signal and Image Processing: An International Journal (SIPIJ)*, vol. 2, no. 2, June 2011.
- [8] M. U. Celik, G. Sharma, and E. Saber, "Hierarchical watermarking for secure image authentication with localization," *IEEE Transactions on Image Processing*, vol. 11, no. 6, pp. 585-594, June 2002.
- [9] F. Peticolas, "Information hiding techniques for steganography and digital watermarking," Stefan Katzen-Beisser, Artech House Books, ISBN 1-58053-035, December 1999.
- [10] L. Xie and G. R. Arce, "A class of authentication digital watermarks for secure multimedia communication," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1754-1764, November 2001.
- [11] M. Barni, F. Bartolini, R. Caldelli, A. De Rosa, and A. Piva, "A Robust Watermarking Approach for Raw Video," In *Proc. of 10<sup>th</sup> International Packet Video Workshop PV2000*, Cagliari, Italy, May 2000.
- [12] A. Eskicjoglu and E. Delp, "An overview of multimedia content protection in consumer electronics devices," In *Proc. of Signal Processing Image Communication 16 (2001)*, pp. 681-699, April 2001.
- [13] G. L. Friedman, "The trustworthy digital camera: restoring credibility to the photographic image," *IEEE Transactions on Consumer Electronics*, vol. 39, no. 4, pp. 905-910, November 1993.
- [14] C.Y. Lin and S.F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11, no. 2, pp. 153-168, June 1999.
- [15] C.S. Lu and H.Y. Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme," *IEEE Transactions on Multimedia*, vol. 5, no. 2, pp. 161-173, June 2003.
- [16] X. Tangl, Y. Niu, H. Yue and Z. Yin, "A Digital Audio Watermark Embedding Algorithm," *International Journal of Information Technology*, vol. 11, no. 12, pp. 24-31, June 2005.
- [17] C. Y. Lin, "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection," PhD thesis, Columbia University, 2000.
- [18] V. Yadav and N. Verma, "Secure Multimedia Data using Digital Watermarking: A Review," *International Journal of Engineering Research and General Science*, vol. 4, no. 1, pp. 181-187, January-February 2016.
- [19] M. Ahmed and M. S. Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping," *International Journal on Computer Science and Engineering*, vol. 2, no. 1, pp. 46-50, January 2010.
- [20] Suma, V. "A Novel Information retrieval system for distributed cloud using Hybrid Deep Fuzzy Hashing Algorithm." *JITDW 2*, no. 03 (2020): 151-160.
- [21] Al-Haj, Ali. "Combined DWT-DCT digital image watermarking." *Journal of computer science* 3, no. 9 (2007): 740-746.