Efficient Watermarking Technique using DWT, SVD, Rail Fence on Digital Images

Chirag Sharma
Assistant Professor
Department of CSE,
Lovely Professional University,
Jalandhar, India

Anshu Sharma
Assistant Professor
Department of CSE
CT Group of Institutes,
Jalandhar, India

ABSTRACT

This paper presents an efficient watermarking technique based on Discrete Wavelet Transformation (DWT), Singular Value Decomposition (SVD) and Rail Fence methods that are applied on grey scale and digital color images. First of computation of 10's complement and rail-fence method is applied on watermark image that results in modified watermark image. The singular values of a modified watermark image are embedded in singular values of the LL1 sub-band coefficients of the host image by using scaling factors. Thus as a result the robust watermarking scheme is used to provide security to the watermark image. This proposed method will helpful for copyright protection and ownership identification. This approach leads to secure transmission and broadcasting of digital data.

Keywords

Discrete Wavelet Transform, Singular Value Decomposition, Rail-Fence, 10's compliment

1. INTRODUCTION

Widespread expansion of internet has led to the available of digital data in the form of images, videos and audio. This has lead to the problem of copyright protection. Digital watermarking is a technique to protect digital media. It is a technique that is used to embed secret information into the digital content; same information may be in the form of text, image and is embedded into digital media The main reason of using these watermarking techniques is to secure or protect the digital content (image, text, audio or video) and enable copyright protection. Now a day's multimedia technology has been grown very fast and for secure digital data transmission so we need some special mechanisms like digital watermarking and Data Hiding. The audio and video files that are available at free of cost in websites but not secure. Watermarking technique will protect digital content in such a way that it will give protection during its (watermark) entire lifespan. Watermarking techniques will also provide the ownership identity, proof of ownership [1]. Digital watermark is added to the legal copy such that it will protect the copyright of the digital content. It is of 2 types: Visible and invisible. Several mechanisms existed in digital watermarking are:

A. Embedding process: It is performed in between the digital content and watermark data (image, audio or video) and the result will give the watermarked digital content and the other side the detection action will be performed. It can be done in visible and invisible manner.

B. Extraction process: To get the watermark image inverse embedding mechanism is performed on the watermarked image.

2. EXISTING SYSTEM

Anurag Mishra, 2014- This paper describes optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. This Watermarking technique had mainly focused on two terms such as Robustness and Imperceptibility. Normally in digital watermarking the watermark should always remain with the Host image and this system has provided a robust algorithm. In this paper the technique applied black and white image as the watermark image and it was found the singular values of it. Host image or original image as grey scale image and they calculated 3-level DWT of it and then found singular values LL-3 sub band of the image. The singular values of a watermark image are embedded in singular values of the LL1 sub-band coefficients of the host image by making use of scaling factors will gives the watermarked image. if an attacker knows the SVD and DWT algorithm then he will easily detect the watermark image. This is one of the limitations of the existing approach [1]. Here brute force attack mechanism is applied to further check performance of proposed watermarking technique.

3. PRESENT WORK

The digital watermarking contains two types of algorithms embedding and extraction algorithm. This proposed system used four methods that are SVD, DWT, 10's complément and rail-fence and brute force attack.

3.1 Singular Value Decomposition (SVD)

This is one of the numerical analysis techniques that decomposes an image into different levels. In the earlier days it had worked only on the square images but now the technology has improved so it is useful even for the rectangular images. SVD method has been used in many applications such as image watermarking, image hiding, image compression and noise reduction.

Consider an image N×N size represented with A and it has been decomposed into the following

A= UA*SA* $(VA)^T$ = $\sum_{i=1}^{r} ui * si * (vi)^T$ where UA = [u1, u2, u3….uN]

VA = [v1, v2…….vN]

$$S=\begin{pmatrix} s1 & \cdots & N \\ \vdots & \ddots & \vdots \\ 0 & \cdots & sN \end{pmatrix}$$

UA and VA are the N×N Orthogonal Matrices and S has Singular values from (s1, s2,…sN) and singular values follows decreasing order from top to bottom. This method has used for the Host image and watermark image.

3.2 Discrete Wavelet Transformation (DWT)

Wavelets depends upon two parameters such as scaling and shifting. In real world signal process is used to work on discrete signal not on the continuos signal. Wavelet is used perform transformation and inverse transformation by using two banks of filters that are analysis filter and synthesis filter. Analysis and synthesis filters are used for forward and reverse transformation. In this existing scheme host image will act as 2-D Signal. When the 2-D signal goes to the analysis signal in case of 1-level of decomposition the signal becomes ¼th of the original signal that will give four sub bands (LL1, LH1, HL1 and HH1) with different resolutions then SVD will be applied on LL1 sub band coefficients and embed the watermark image (singular values of modified watermark image). This DWT has been used in many applications such as image compression, digital watermarking and noise reduction etc. This method is only used for host image in the existing and proposed systems [1]

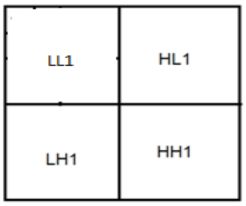


Fig 1.1: 1-level Decomposition of an Image

3.3 10's Complement

Calculation of the 10's Complement of the watermark image pixel values is done by following example.

Example: 10's Complement of 233

(9-2) (9-3) (9-3) = 766

Then add 1 766+1=767 (it is 10's Complement of 233).[1]

3.4 Rail Fence Method

It is the basic Transposition technique which will be used to Encrypt and Decrypt the given input data without using any key. The attacker can easily break this algorithm but this algorithm can be applied on the tens complement data that is a secure scheme.

Example: input: she is watching, encrypted text as follows:

s e s a c i g
h i w t h n

Encrypted data is: sesacighiwthn.

These two methods (10's complement and rail-fence) have been applied on watermark image so that;it will increase the imperceptibility of the watermark image when it is compared with the other methods. The DWT and SVD methods have been used as similar in the Existing and Proposed Systems.

The proposed method has two algorithms such as

i. Proposed Embedding Algorithm

Step 1: First apply the 1-Level DWT method on the Host Image by using the HAAR filter and obtain the LL1 sub band coefficients of it (Size of m×m).
Step 2: Then apply SVD method on the LL1 Sub band Coefficients of the Host image. To calculate it the formula is: [U, S, V] = SVD (LL1)
Step 3: Apply 10's Complement on the Watermark Image (w) and get the image 'w1'.
Step 4: Apply Rail fence encryption algorithm on the 10's Complement Watermark Image (w1) and get the modified watermark image (wc).
Step 5: Apply SVD method on the modified watermark image (wc). To calculate it the formula is: [Uw, Sw, Vw] = SVD (wc)
Step 6: Embed singular values of wc into the singular values of the LL1 sub band (Embed Sw into S). To calculate it the formula is: S'=S+(δ*Sw)
Step 7: Get the Adapted LL1 Sub band coefficients LL3' by using the LL3' = (U * S' *$(V)^T$)
Step 8: Apply the 1- level IDWT method and to get the Watermarked Image[1].

ii. Proposed Extraction Algorithm

Step 1: Apply 1-level DWT method using the HAAR Filter on the Host Image i and the watermarked Image i' to get the LL3 and LL3' sub band Coefficients which consists the size of m×m.

LL1=DWT (i) and LL1'=DWT (I')

Step 2: Then apply SVD method on LL3 and LL3' Sub band Coefficients by using the formula:

[U, S, V] = SVD (LL1) and [U', S', V'] = SVD (LL1').

Step 3: Calculate the singular values of the Watermark Image by Using Swc' = [S' – S]/δ.

Step 4: Recover or extract the Watermark by using this Formula: (wc)' = Uw * Swc' * $(V)'$

Step 5: Decryption is applied of Rail fence to the (wc)'.

Step 6: Inverse of 10's complement is applied to the output of above step and Extract the Watermark Image w'[1].

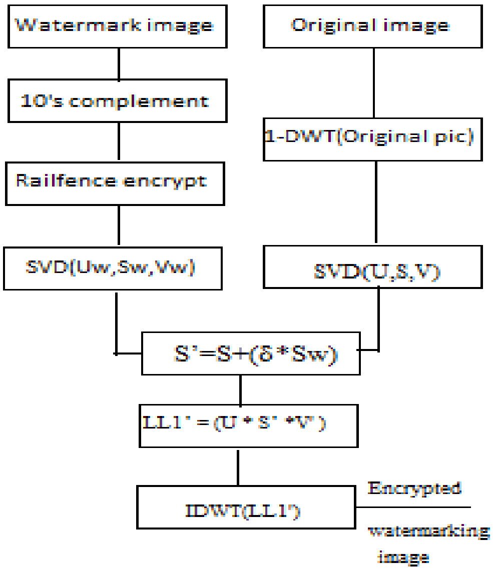


Fig 1.2: Proposed Watermark Embedding process[1]

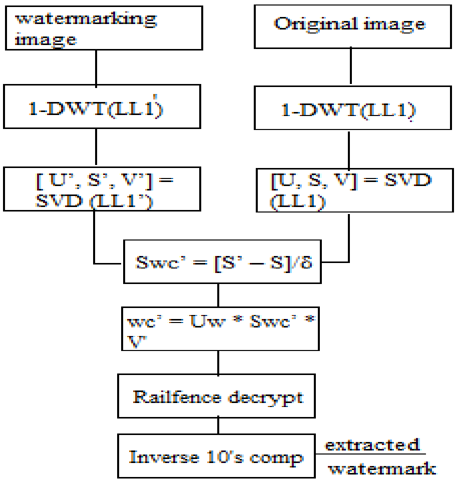


Fig 1.3: Proposed Watermark Extraction Process[1]

iii. Process of original image extraction

The process of original image extraction is given below

Step1: Consider watermarking image (oi) and extracted watermark image (ew).

Step2: Apply 1-DWT on watermarking image and then apply SVD (LL-1) sub band.

Step3: Apply 10's complement and rail-fence on extracted watermark image and got ew' then apply SVD (ew') of it.

Step4: Singular values of original image will be calculated by using the below formulae

Snew=s(LL-1)-s(ew')* δ

Step5: The original-image is calculated by formula=U*Snew*V'.

Step6: IDWT is applied on(original-image) and it gives the Extracted original image [1].

4. RESULTS AND DISCUSSION

The existing method have used grey scale image for original image and black and white image for watermark image but the proposed method used the grey scale images (both for original and watermark image) and Digital color images(both for original and watermark image). In the both the cases it provided good results in case of PSNR it means good quality of output image and the NC. The results are analyzed by using in MATLAB.

4.1 Grey scale images

4.1.1 Watermark embedding algorithm on grey scale images

Consider 256×256 size original image and 128×128 size watermark image (both are grey scale images). First we calculate 10's complement on the watermark images and it provided us with 10's complemented images. The range of grey scale image is 0-255. Whenever we perform 10's complement on the grey scale images after some time it may exceed the range, for example consider any pixel value as '100' by performing 10's complement on this it gives the result as 900. It has given the result that was not in the range on such numbers Then modulus function was performed with 255 so that the pixel value will become within a range of required result. Rail fence method has been applied on the 10's complement images and it has given an encrypted image. After this SVD is performed on an image to get singular values of the encrypted watermark image. After completion of this work original original imag is taken and calculated LL-1 band of it by applied DWT. Harr filter has used for it. Calculation of the SVD(LL-1) band and given the singular values is done. The encrypted watermark image singular values is embedded in LL-1 singular and gave the new singular values (snew) by using the formulae snew=s+(δ *sw). where s= singular values of orginal image (LL1) and sw=singular values of encrypted watermark image). After this H=U*snew*V' is performed that will give the inverse of SVD. Whenever we performed IDWT on this images (H) ,watermark image is taken as result.

In this experiment,original image is taken as Nature and watermark image is taken as bird.

4.1.2 Watermark Extraction algorithm on grey scale images

DWT of the both the images is calculated which gives the LL1 (original-image) and LL-1 (watermarking image).The singular values of the both the LL1 band images are calculated. S1=singular values of original image (LL1) and S2=singular values of watermarking image (LL1). Snew=(S2-S1)/ δ from this formula we grab the new singular values of watermark image (Encrypted).An inverse operation of rail-fence and inverse of 10's complement is applied to the extract watermark image with good visibility as a result.

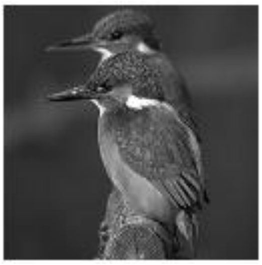


Fig 1.4: Watermark image.

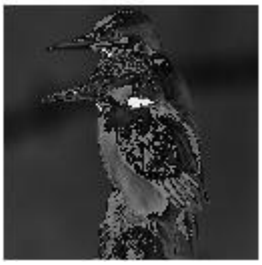


Fig 1.5: 10's comp image

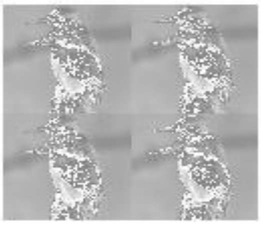


Fig 1.6: Rail-fence on 10's complemented image

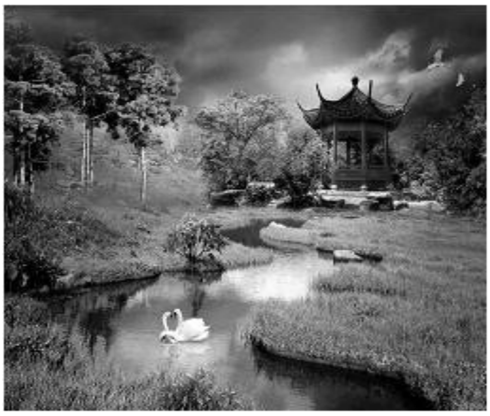
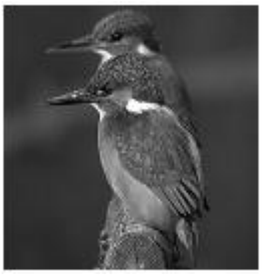


Fig 1.7: watermarking image



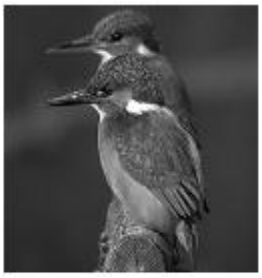


Fig 1.8: watermark image Fig 1.9: Extracted watermark image

The above results showed that, this proposed method provides robustness (quality of watermark image and extracted watermark image is similar) and as well as security (by using 10's complement and rail-fence method). This proposed method has also been applied on various images such as Baboon, Boat, Cameraman, Bird, Barbara and Peppers and got good results in case of PSNR and NC. Nature image is original image for every image.

5 PSNR AND NC VALUES

The PSNR and NC values of proposed work cannot be compared with the existing method because of change in the data set. The existing method had used grey scale image for original image and black and white image for watermark image but the proposed method used the grey scale images (both for original and watermark image) and digital color images(both for original and watermark image). But still the proposed method has provided good PSNR and NC values. It provides good result (good PSNR and NC values), whenever our δ=0.05, 0.005 and 0.1.

This is the formula to calculate the PSNR value:

PSNR=10 $\log_{10}(\frac{\text{Imax}^2}{\text{MSE}})$ where Imax is the maximum possible pixel value of the Image 'I' and MSE is the Mean Square Error. If the value of the PSNR is more, then the quality of the image is more and the lesser is the Error rate of the image.

To calculate the Normalized cross correlation (NC) the formula is:

$$\text{NC (w, w')} = \frac{\sum_{i=0}^{m} \sum_{j=0}^{n}[w(i,j),w'(i,j)]}{\sum_{i=0}^{m} \sum_{j=0}^{n}[wc(i,j)\ast wc(i,j)]}$$

Where w(i,j) is original watermark image and w'(i,j) is the extracted image.

Table1: PSNR and NC (w,w') between watermark image and extracted watermark image of the proposed work.(For grey scale images)[1]

Image	δ=0.05	δ=0.005	δ=0.1

Nature with Baboon	PSNR=35.00
	NC=0.95
		PSNR=39.00
		NC=0.97
			PSNR=40.12
			NC=0.98

Nature with Boat	PSNR=39.12
	NC=0.98
		PSNR=36.35
		NC=0.96
			PSNR=39.00
			NC=0.978

Nature with Camera-man	PSNR=35.24
	NC=0.967
		PSNR=37.56
		NC=0.971
			PSNR=39.02
			NC=0.98

Nature with Bird	PSNR=37.00
	NC=0.97
		PSNR=36.01
		NC=0.96
			PSNR=39.12
			NC=0.99

Nature with Barbara	PSNR=38.00
	NC=0.98
		PSNR=39.23
		NC=0.988
			PSNR=40.23
			NC=0.999

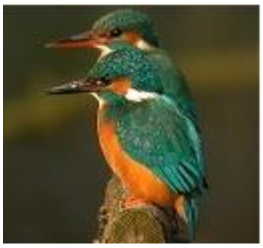
Nature with Peppers	PSNR=35.24
	NC=0.967
		PSNR=34.78
		NC=0.957
			PSNR=36.22
			NC=0.96

From the above figure it has been concluded that proposed method has given good PSNR and NC values. This proposed method also showed that it has provided robustness from the above results. The loss of data is very less in the proposed method.

5.1 Digital Color Images

The process of embedding and extraction in grey scale images and digital color images are same. The difference between is the dimensions. But a grey-scale image has two dimensional sizes where digital color image has three dimensional sizes. The time complexity and space complexity of the digital color images are more when it is compared with grey scale images. When 10's complement is performed on the watermark image then the modular operation (with 255) is applied on the pixel values which has more than 255 value. By the complexity of the process reduces, Remaining all process of this embedding and extraction of Digital color images same as grey scale images (same as the above). 10's complement is applied first and rail-fence encryption on the watermark image that will give the encrypted (modified) watermark image. When the embedding process is done for both encrypted watermark image and for original image the separation of RGB components of the both the images [1]. For example the red components of the encrypted watermark image will be embedded in red components of original image, the green components of the encrypted watermark image will embed in green components of original image and the blue components of the encrypted watermark image will be embedded in blue components of original image.

Nature image is taken as original image and Bird as the watermark image.



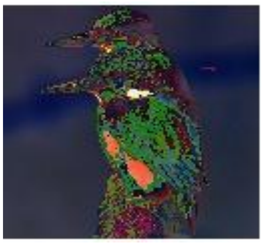


Fig 1.10: watermark image Fig 1.11: 10's comp image

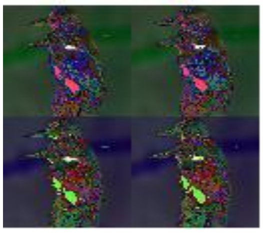


Fig 1.12: Rail-fence of 10's complemented image

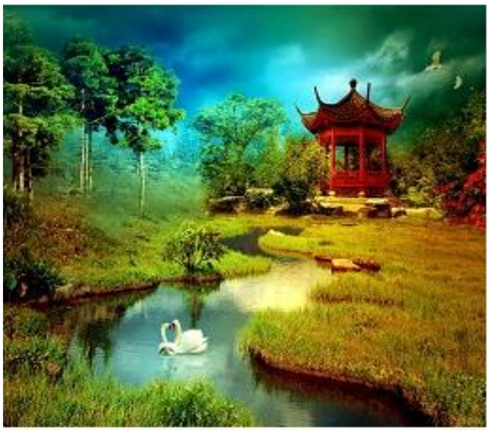
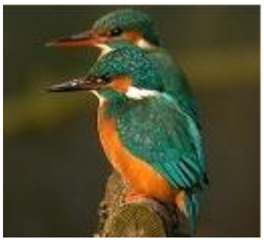


Fig 1.13: **Watermarking image**



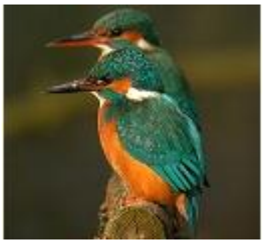


Fig 1.14: Watermark image   Fig 1.15: Extracted watermark image

The above figure has shown that the watermark has been extracted without less amount of loss. So this algorithm has also been working efficiently for digital color images. It has also provided good PSNR and NC results.

Table2: PSNR and NC(w,w') between watermark image and extracted watermark image of the proposed work.(For digital color images) where Nature is the original image.

Image	δ=0.05	δ=0.005	δ=0.1

Nature with Baboon	PSNR=42.22
	NC=0.98
		PSNR=42.15
		NC=0.97
			PSNR=44.14
			NC=0.99

Nature with Boat	PSNR=39.12
	NC=0.96
		PSNR=44.14
		NC=0.99
			PSNR=43.33
			NC=0.98

Nature with Camera-man	PSNR=41.22
	NC=0.98
		PSNR=43.15
		NC=0.98
			PSNR=40.25
			NC=0.97

Nature with bird	PSNR=44.10
	NC=0.99
		PSNR=43.90
		NC=0.989
			PSNR=42.14
			NC=0.998

Nature with Barbara	PSNR=43.65
	NC=0.99
		PSNR=39.54
		NC=0.96
			PSNR=41.32
			NC=0.98

Nature with Peppers	PSNR=44.12
	NC=0.998
		PSNR=43.65
		NC=0.99
			PSNR=39.69
			NC=0.96

From the above figure it has concluded that our proposed method has given good values PSNR and NC values. This proposed method also showed that it also provides robustness from the above results. The loss of data is very less in the proposed method. This digital color images has given the good visibility to the viewers when it will compare with the grey scale or black and white images. So from the above table we got good efficient values of PSNR and NC values for almost every image that has been used in the table.

5.2 Extraction of the original image (color image)

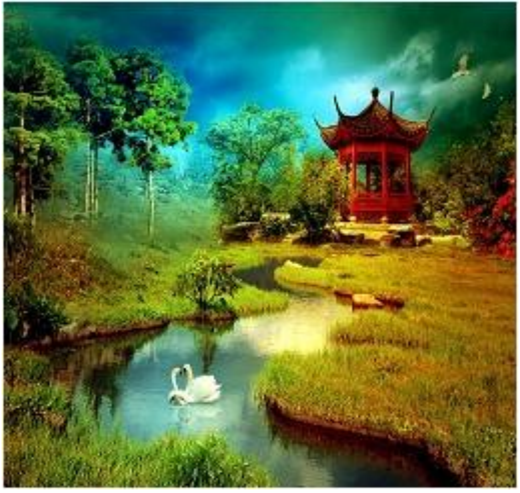


Fig 1.16: **Original imge**

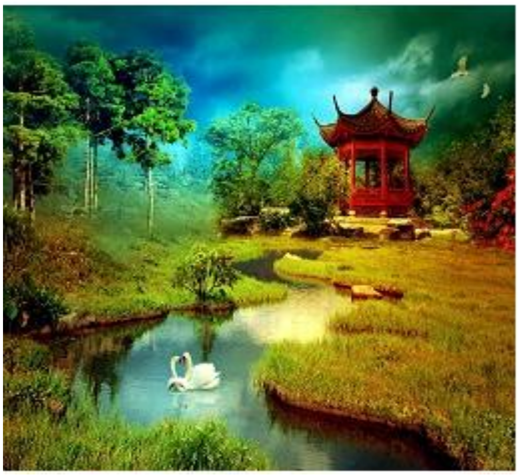


Fig 1.17: **Extracted original image**

From the above figures the conclusion was made that both images are also looking like same so there is less loss of data. From this it is concluded that this proposed method efficiently working for both grey scale images and as well as digital color images. This proposed method have also provided security against various types of images processing attacks such as JPEG 5%, Histogram equalization and sharpening on both the grey scale and digital color images.

Table 3: Comparison of NC (w,w') value in case of different image processing attacks (on digital color images only). These values are noted in the presence of δ value equal to 0.1

Images	JPEG 5%	Histogram equalization	Sharpening
Nature with Baboon	0.95	0.968	0.76
Nature with Boat	0.97	0.98	0.69
Nature with Cameraman	0.925	0.976	0.82

Nature with Bird	0.965	0.966	0.98
Nature with Barbara	0.92	0.97	0.92
Nature with Pepper	0.96	0.963	0.88

From the above table the conclusion was made that there is only some significant loss and that loss cannot effect the visual quality of the data and moreover it has been providing more security in case of image processing attacks. But when sharpening attack is performed then NC value is reduced.

5.3 Performing brute force attack on digital color image

When attacker wants to perform brute force attack on an image (after applied derail-fence algorithm) then he won't get the exact image. First he observes the pixel values of the data and then he performs the attack with some possible values.

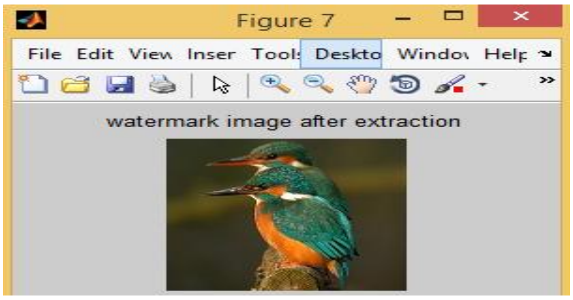


Figure 7
File Edit View Inser Tool: Deskto Windo Help
watermark image after extraction

Fig 1.18: Extracted watermark image

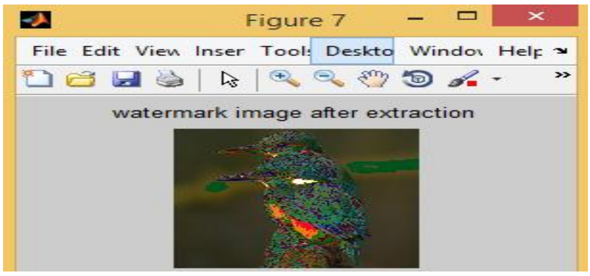


Figure 7
File Edit View Inser Tool: Deskto Windo Help
watermark image after extraction

Fig 1.19: **Extracted watermark (after brute force attack)**

When extraction of watermark image is done (w/o brute force attack) then the PSNR and NC value of the above bird image (Fig 1.18) will be 43.722 and 0.9996. but when attacker wants to perform brute attack on the image (after derail-fence process) then he will get this bird image(fig 1.19). The PSNR and NC values of the attacked image are 16.32 and 0.66 so from the above two figures it can be concluded that the extraction process is very difficult for the attacker.Attacker looses main information of watermark image after brute force attack Hence the proposed algorithm gives more security in an efficient manner.

6 SUMMARY AND CONCLUSION

The main advantage of this proposed approach is to maintain robustness and security the watermark image. Time and space complexity was low for grey scale images. Visible quality of an image will increse in case of Digital images.It provides security against active and passive attacks in the network. It will be concluded that the security of the proposed method is getting affected in the given scenario: considering two pixel values 99 and 9, the 10's complement of these pixel values will be 1 and 1.So in such case it is mandatory to have the inverse 10's complement algorithm then only it gives correct results. So this algorithm will provide security to the present system and the inverse process of this 10's complement will be somewhat difficult to trace for the hacker.

Table 4: 10's complement results

Pixel values	10's complement
9	1
99	1

Advantages of using 10's complement and rail-fence method with an example: This proposed method has used the 10's complement that provides security to the watermark image. Analysis of the exact pixel value of the watermark image after applying 10's complement on it becomes very difficult. The below example will show another advantage of the 10's complement. Let us consider one pixel value of the grey scale watermark image as '10'. After application of 10's complement on the pixel value provides the result as 90. In the above example 10 became 90 so there is much difference in between 10 and 90. By using this method it is very difficult for the attacker to get the exact image due to the massive variation in the pixel values before and after application of attack. The proposed method has the mixture of 10's complement and rail-fence method these two methods provides the security to the watermark image. The rail-fence method provides security against active and passive attacks. But the experiments have shown that this had destroyed by the attackers in the earlier days. If it has combined with the 10's complement then definitely it will become one of the better approaches for securing the image. Whenever 1's complement and 2's complement were applied on the image pixel values the pixel values became almost similar comparision is done with the original pixel , by using 10's complement it has became much difference In the original pixel value and the after 10's complemented pixel. So it has provided more security when it compared with the 1's complement and 2's complement [1].

Table 5: 10's complement comparison results[1]

Complement method	Original pixel value	Pixel value after applied complement method
1's complement	10	5
s2's complement	10	6
10's complement	10	90

From the above figure it has been concluded that whenever 10's complement has used the pixel value will become drastic change. From this it has been concluded that this proposed method has provided robustness and security in an efficient way. This proposed algorithm has been used on both grey scale image and digital color image where as existing system only worked on grey scale. It has given good PSNR and NC values even after applied some types of image processing attacks.

7 FUTURE WORK

Sometimes the attacker may be get an original pixel values easily if he will perform brute force attack but that is definitely going to take some time to get the original pixel values. If the best security algorithm like symmetric algorithms such as DES and AES are used ,it will increase the security of the watermarking technique. The PSNR and NC values of the proposed method has given the good results.

Further this technique can be applied on videos.Video is a collection of frames that are colored images. The Future of the proposed technique can be implemented in raw and compressed Videos as it is applicable for colored images.

8 REFERENCES

[1] C.Sharma, K. Shylesh," Efficient Watermarking Technique using DWT, SVD, Rail fence and 10's complement applied on Digital Images",IJAER,Vol-**10(55**),2015.

[2] A. Mishra , C. Agarwal , Arpita Sharma, Punam Bedi (2014), "Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm".

[3] B. Gunjal, Dr. S N Mali (2012), "a survey on Applications of Digital Image Watermarking in Industries".

[4] L. Hui-fang, C. Ning, Chen Xiao-ming (2010) "A study on image digital water-marking based on wavelet transform".

[5] M. Tong, T. Chen, Wei Zhang, Linna Dong (2003), "New Video Watermark Scheme Resistant to Super Strong Cropping Attacks"

[6] M. Ghobadi (2006), "A survey on wavelet-based coding and its application in JPEG2000".

[7] N.Singh, A. Nandi (2004), "Digital water-marking mark This Technology".

[8] P. D SHUKLA (2003), "complex wavelet Transform and their applications" pg: 25-55.

[9] P. Singh, R S Chadha (2003), "A survey on Digital Watermarking Techniques, Applications and Attacks".

[10] S. Bhattacharya, T Chattopadhyay, Arpan Pal (2006),"A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC".

[11] Z. J Xu, Z Z Wang, Q Lu (2011) "Research on Image Watermarking Algorithm based on DCT"