

A Robust Histogram Shape-Based Approach for Image Watermarking Using Artificial Neural Network with Optimization

Amandeep Kour and Simrandeep Singh
Department of Electronics and Communication Engineering, Chandigarh University,
140413 Gharaun, Punjab, India

Abstract: A scheme for creating digital image copyright certainty is presented in this research with histogram shaped based on artificial neural network. The proposed work watermarking is based on visual key based utilizing genetic algorithm and artificial neural network. The proposed system is going on the adoption of random pixels from the original digital image rather of a particular election of pixels. In today's outline certainty of digital data is utmost essential in every part of life. More sound methods are being developed to shield the proprietary claims of the multimedia. In this study, an invisible watermarking technique is performed to embed various binary watermarks into digital images based on the idea of cryptography. The proposed project embeds the watermarks without altering the original cover image. In proposed work, we perform the very user-friendly and robust histogram shape-based program for image watermarking using Artificial Neural Network with optimization. For the assortment of the suitable domain from the cover image, we practice Artificial Neural Network (ANN) but there are one more obstacles occurs during an assortment of a suitable region from the cover image to embed the message data. The difficulties are optimization if we cannot use optimization technique then we got the space with disturbance. So, for the optimization, we use a Genetic Algorithm (GA). The foremost developments in the research are genetic algorithm. Experimental outcomes show the recommended work can recover the watermark pattern from the marked image even if significant changes are performed to the original digital image. The image watermarking is executed using image processing toolbox within MATLAB Software.

Key words: Copyright, digital image, digital watermarking, histogram, genetic algorithm and artificial neural network, software

INTRODUCTION

Digital watermarking is signified as an algorithm that can be prepared to conceal secret data into digital audio, video, image or documents in an appearance that does diminish the overall property of the original cover signal. The primary data is named as 'cover data' or 'host signal'. The means of inserting the secret data is described as embedding and the image after embedding is called "watermarked image". Extraction or detection is a manner retrieves the stored watermark. Thus, the pair of principal mechanisms of digital watermarking schemes is embedding and extraction. The watermarking methods are grouped as text-based watermarking (Li and Dong, 2008), image watermarking, video watermarking, audio watermarking and 3D watermarking (Jalil *et al.*, 2010). Due to advancement in information and communication technologies, digital evidence (such as image, video, audio or text) can be easily distributed, duplicate and modify.

In proposed activity, digital image watermarking approach has been developed to preserve the reflective

property of image in digital form based on histogram method. Data concealing relates with communication of data by concealing in and later recovering it through any digital cover media form. The digital cover media can be a photograph, audio-visual, an audio or solely a common text document. Data hiding is a broad term covering many sub-classifications. There are three ways: cryptography, watermarking and steganography.

Cryptography deals with encryption and decryption (Saha *et al.*, 2014) of data, although, its presence cannot be hidden from the third person. Watermarking is not a different system, it just alike as cryptography and we also combining the cryptography and watermarking (Thapa *et al.*, 2011) for more security purpose.

Watermarking intends to keep the existence of the message (in image, video, audio, text etc) secret in the cover image. The watermarking mode comprises three important components the data to be hidden (here, image), the cover file and the resulting stego file (after embedding the secret image within a cover file).

Figure 1 shows the process of watermarking in which there is cover image on which secret image has to be

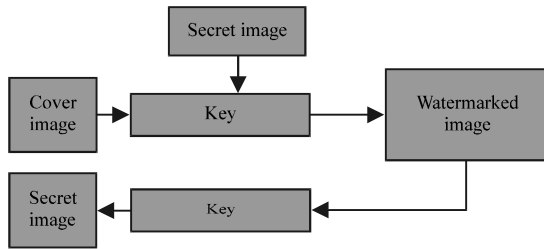


Fig. 1: Watermarking process

embedded then with the help of key is sent over a transmission medium, then on the receiver side, the decoder is there to extract the secret image.

In this study, we have prearranged for a concise summary about the proposed histogram shape based watermarking model with optimization and artificial neural network in which the embedding and extracting algorithms is fully based on the relevant classification of pixels bits. The watermarking technique proposed in this research may be very effectual against different low-frequency an attack that demolishes the low-frequency constituent of the image.

Li and Dong (2008) presents an innovative text watermarking achievement but for the Chinese text merely. In his or her opinion he's mentioned this some bit stream prototype of the text on the basis of which the merging can be done. His approach also describes the pictographic approach of the text and the illustration probably of the person. This method will be despite the fact that comes with a useful thinking but the predicament is as the Chinese language is so complicated, it fits there but not with each and every specification. His/her algorithm may be intended particularly for Chinese characters and hence, this algorithm cannot be used for global language. Jalil *et al.* (2010) presented a zero text watermarking scheme in the international conference of 2010. According to them, existing text watermarking algorithms are not robust against random insertion and deletion attacks on the selective text document. By means of growing strength of the attack, the permanence of the watermark in the text document turn out to be challenging and hence, they revealed a unique text watermarking algorithm that can be used for copyright protection of textual substances. They will when matched their results along with various other existing algorithms of the same contrast and their results are found to be effective enough to get proceeded for modification. Mali *et al.* (2013) performed a watermarking scheme on the basis of neural networks. It was an incredible initiative to include neural networks into the contrast associated with encryption. The neural network generates the weight for each and every input contributed to it rather than taking everything as an input stream. The pattern changing of the neural network is considerably comparable to

SVM as it also converts the complete input according to its oversimplification and then precedes. Hence, his approach is considerably effective and can be considered for the future development process.

MATERIALS AND METHODS

To authenticate the effectiveness and accuracy of propose robust histogram shape-based method for image watermarking using artificial neural network with optimization, we perform several experiments with this procedure on several images. In proposed work, several steps will use to select the appropriate pixel region to embed the secret message and enhance the image watermarking process. The methodology of propose work is given as follows.

Step 1: Design and develop a proper GUI of propose image watermarking module.

Step 2: Develop a code to upload cover image and secret image from database for training and testing.

Step 3: Apply pre-processing on uploaded cover and secret image. In pre-processing step, we apply the some basic process like filtering, resizing, conversion, etc. to make the uploaded image useful.

Step 4: Develop a code for the histogram construction of cover image and initialized the genetic algorithm for the optimization of histogram pixels.

Step 5: After that set the fitness function of Genetic algorithm according to the requirement, so, we can find out the appropriate and optimal pixel group.

Step 6: Initialized artificial neural network with pixels group of cover image as an input of artificial neural network. Train artificial neural network using cover image pixel groups and according to training find out best and appropriate region of that pixel by using this we can embed the secret image, so, the information losses should be less as compare to the existing work.

Step 7: After that generate a private key to embedding process.

Step 8: Embed the secret image in cover image using their suitable region with the private key.

Step 9: After the embedding phase extraction part enable and we extract the secret image from the cover image using private key and if key is correct then, we got the secret message otherwise, we cannot extract the secret image.

Step 10: At the last, we compute the performance metrics like MSE, PSNR and SSIM.

MSE: In statistics, the mean squared error of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated:

$$MSE = (1/N) \sum |x(i) - e(i)|^2$$

Where:

x and e = The original and restored image, respectively

N = The number of pixels in the image

PSNR: Peak Signal-to-noise Ratio, often abbreviated PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The Peak Signal-to-Noise Ratio (PSNR) is defined as:

$$PSNR = 10 * \log(255 * 255 / MSE)$$

Entropy: The entropy is a valuable tool to measure the richness of the details in the output image. By using given formula we calculate the entropy of original and enhanced image:

$$Entropy = \text{Summation}(p_i * \log_2(p_i))$$

Figure 2 shows the flow chart of proposed work for the robust histogram shape-based method for image

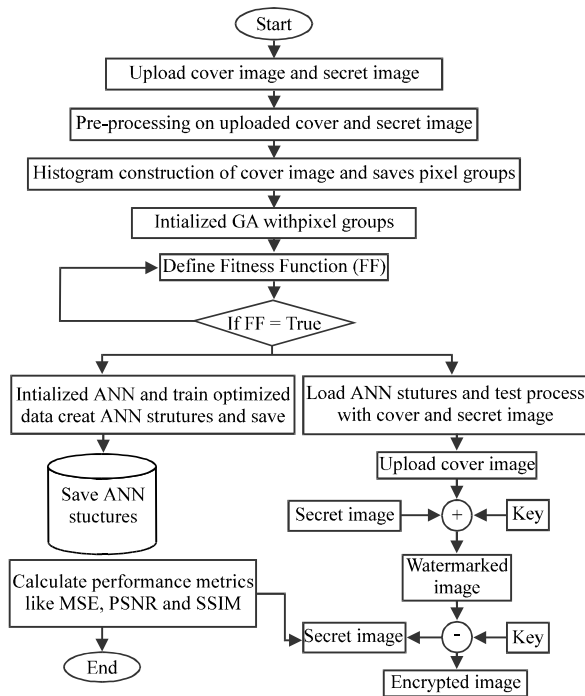


Fig. 2: Flow chart of proposed work

watermarking using artificial neural network with optimization. By using above procedure we achieve better results which are well described in the next study.

RESULTS AND DISCUSSION

In this study, we describe the simulation of proposed work with results. There are some algorithms which are used in the proposed simulation work:

Algorithm 1; Embedding algorithm:

```

Upload cover image and secret image
Apply pre-processing on uploaded cover image as well as secret image
Find out the histogram using HSBM
Initialized genetic algorithm
Define the population size of the GA (50)
Load Pixel set sets
for I = 1 to all Pixels
    for r = 1 to all rows (Pixels)
        for c = 1 to all columns (Pixels)
            Define Ft (Threshold) = Average of Pixels value
            Define Fs = Pixels (r, c)
            Call fitness function
            Fit_data = Fitness functions (Ft, Fs)
            If fitness functions == true
                Fit_data = Fs
            else
                Fit_data = Ft
            Consider as best solution of GA and store as GA_data
        end
    end
end
end
Save all GA data for training of artificial neural network
Initialize ANN
Generate group of data = group
Set iteration = 50
For I = 1 to iteration
    Weight = pixels
    Hidden_Neurons = (Santhi and Thangavelu, 2009) (tansig)
    Net_algo = trainlm
    Generat Net structure of ANN (net)
    Net = train (net, Training_data, group)
    Pixles_region = sim(net, Training_data)
End
Train GA data and find region to embed the secret message
Insert key
Apply embedding
Save watermarked image
    
```

Algorithm 2; Extraction algorithm:

```

Load watermarked image
Insert key
If key is matched
    Secret image extracted
    Calculate parameters
else
    Encrypted image extracted
    Calculate parameters
end
Initialize different types of attacks like
For watermarked image
1. for Noising
2. for Filtering
3. for Cropping
4. for Compression
5. for Rotation
6. for Bending
7. for Scaling
8. for Shearing
    
```

```

    9. for Loop
    10. for Jittering
end
If select any type of attack
    Simulate with attacks
else
    Simulate without attacks
end

```

The detail about the proposed robust histogram shape-based method for image watermarking using artificial neural network with GA optimization techniques is given. The simulation of proposed work is given.

The simulation of the proposed for the robust histogram shape-based method for image watermarking based on the artificial neural network with GA optimization techniques. After the simulation we can calculate the performance metrics like MSE, PSNR and SSIM of extracted image. There is one section given for the simulation performance metrics as a result panel and result panel is activated when we click on the result button. Different types of attackers are in used to check the efficiency of proposed work. In the proposed work, if key is wrong then we cannot extract the exact secret image. The extracted image is encrypted, so, we cannot find out the secret data if we enter the wrong key in proposed work.

Figure 3 shows the attacks in proposed work and there are original image, salt and pepper noise, median filter, gaussian noise, JPEG compression, rotation, bending, scaling, shearing, loop, random jittering, cropping. The results of proposed algorithm are given in below section with parameters.

Table 1 represent the comparison of the performance metrics like MSE, PSNR and SSIM of extracted image for previous work as well as for proposed work. From the table we observed that the performance metrics of proposed work is better than the previous work and we achieve best result without losing the more information from the images.

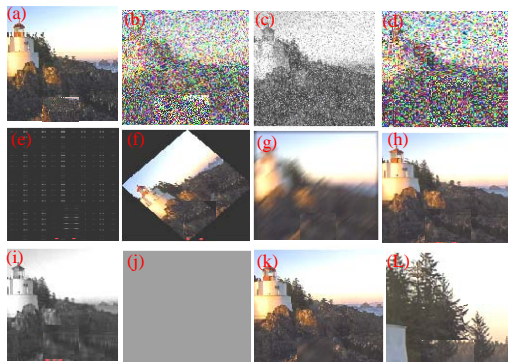


Fig. 3: Illustration of attacks in proposed work

Figure 4 shows the graphical representation of MSE value for proposed work and we compare the proposed MSE with previous work and founded that the proposed MSE is less as compare to the previous work.

Figure 5 shows the graphical representation of PSNR value for proposed work and we compare the proposed PSNR with previous work and founded that the proposed PSNR is better as compare to the previous work by using the artificial neural network with the GA optimization technique.

Table 1: Performance metrics comparison

Previous work			Proposed work		
MSE	PSNR	SSIM	MSE	PSNR	SSIM
0.32	46	0.91	0.017	52	0.93
0.33	43	0.92	0.018	49	0.92
0.43	44	0.93	0.017	48	0.94
0.35	42	0.95	0.019	51	0.95
0.32	45	0.94	0.016	56	0.97
0.34	42	0.95	0.013	54	0.96
0.36	41	0.96	0.012	53	0.93
0.34	46	0.92	0.017	48	0.94
0.38	47	0.97	0.015	51	0.95
0.37	44	0.98	0.021	54	0.95

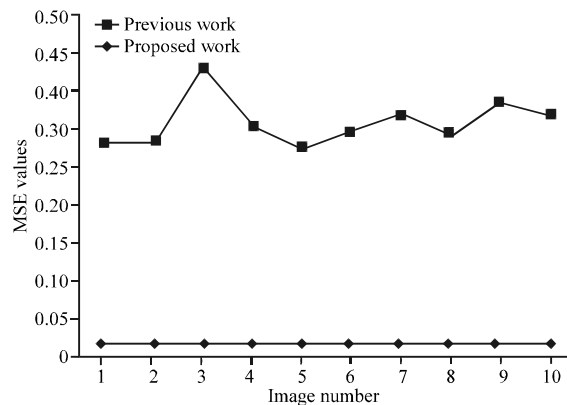


Fig. 4: Simulated window of proposed work

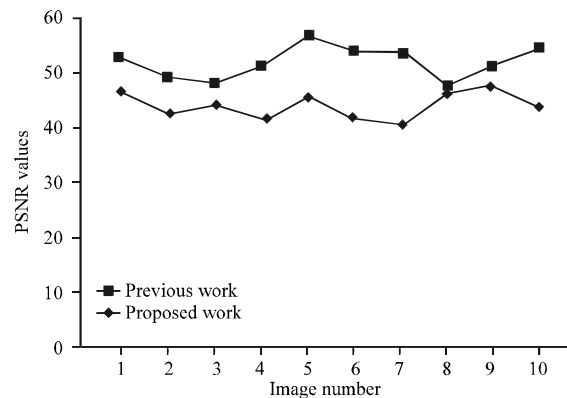


Fig. 5: Simulated window of proposed work

Figure 6 shows the graphical representation of SSIM value for proposed work and we compare the proposed SSIM with previous work and founded that the proposed SSIM is better as compare to the the information loss of proposed work is less as compare to the previous work.

Table 2 and Fig. 7 represents the comparison of the performance metrics like MSE, PSNR and SSIM of extracted image with different types of attacks. There are 10 types of attacks used in proposed work are they are noise, filtering, cropping, compression, rotation, bending, scaling, shearing, loop and jittering.

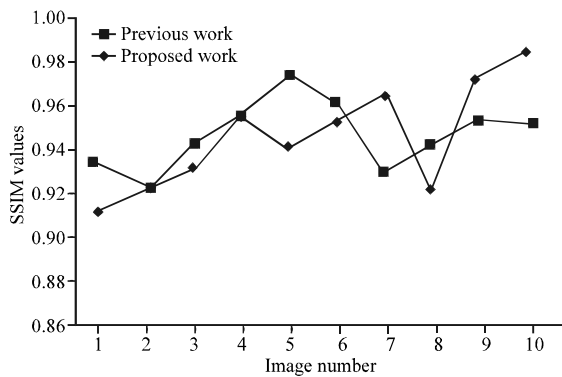


Fig. 6: Simulated window of proposed work

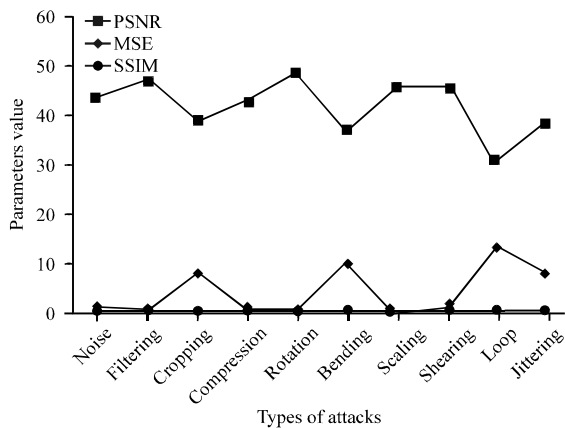


Fig. 7: Parameters comparison with attacks

Table 2: Performance metrics comparison with attacks

Attacks	PSNR	MSE	SSIM
Noise	43.82	0.69	0.91
Filtering	47.27	0.74	0.93
Cropping	39.74	7.48	0.84
Compression	42.89	1.92	0.92
Rotation	48.72	0.58	0.97
Bending	37.91	9.73	0.76
Scaling	46.02	0.94	0.83
Shearing	45.66	1.85	0.94
Loop	31.85	11.64	0.45
Jittering	38.63	8.98	0.59

CONCLUSION

Image watermarking refers to a class of methods that aim to prevent the secret message. In this research, we proposed a novel image watermarking scheme that is robust histogram shape-based method for image watermarking using artificial neural network with GA optimization techniques. In proposed work, we deal with different types of attacks like, noise, filtering, cropping, compression, rotation, bending, scaling, shearing, loop, and jittering. In addition, a protected band is introduced between the selected pixel region to improve the robustness of proposed watermarking technique. In proposed work due to the usage of secret key concept, the proposed watermarking method is also more secure than previous watermarking methods. The superior performance of the proposed watermarking is demonstrated by simulation results. The experimental results analyzed that proposed method using the artificial neural network with GA optimization provides good results having values MSE just near about 0.017, PSNR is more than 50, SSIM is more than 0.90 and entropy is better for restored images.

RECOMMENDATION

In future research, watermarking concept would be presented using the hybridization of optimization technique to achieve the better results.

REFERENCES

Jalil, Z., H. Aziz, S.B. Shahid, M. Arif and A.M. Mirza, 2010. A zero text watermarking algorithm based on non-vowel ASCII characters. Proceedings of the 2010 International Conference on Educational and Information Technology (ICEIT) Vol. 2, September 17-19, 2010, IEEE, Chongqing, China, ISBN:978-1-4244-8033-3, pp: V2-503-V2-503.

Li, Q.C. and Z.H. Dong, 2008. Novel text watermarking algorithm based on Chinese characters structure. Proceedings of the International Symposium on Computer Science and Computational Technology ISCSCT'08 Vol. 2, December 20-22, 2008, IEEE, Shanghai, China, ISBN:978-0-7695-3498-5, pp: 348-351.

Mali, M.L., N.N. Patil and J.B. Patil, 2013. Implementation of text watermarking technique using natural language watermarks. Proceedings of the 2013 International Conference on Communication Systems and Network Technologies (CSNT), April 6-8, 2013, IEEE, Gwalior, India, ISBN:978-1-4799-1710-5, pp: 482-486.

- Saha, B.J., K.K. Kabi, A. Chauhan and C. Pradhan, 2014. A robust digital watermarking algorithm using DES and ECC in DCT domain for color images. Proceedings of the 2014 International Conference on Circuit, Power and Computing Technologies (ICCPCT), March 20-21, 2014, IEEE, Nagercoil, India, ISBN:978-1-4799-2405-9, pp: 1378-1385.
- Santhi, V. and A. Thangavelu, 2009. DWT-SVD combined full band robust watermarking technique for color images in YUV color space. *Intl. J. Comput. Theor. Eng.*, 1: 424-429.
- Thapa, M., D.S.K. Sood and A.M. Sharma, 2011. Digital image watermarking technique based on different attacks. *Intl. J. Adv. Comput. Sci. Appl.*, 2: 14-19.