International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 6, Nov-Dec-2022, ISSN (Online): 2395-566X

Digital Image Watermarking by Select ed Feature of Group Search Genetic Algorithm

Dilesh Khairwar, Asst. Prof. Sumit Sharma
Department of Computer Science & Technology,
Vaishnavi Institute of Technology and Science,
Bhopal, MP, India

Abstract- Image is a proof of any instant happened in the universe. Transformation of image from hard to digital brings different flexibility and uses for the analysis and storage. Digital images need security from the intruder for that many communication protocols were developed. For the validity of authentic source watermarking plays an important role. This paper has proposed a model that embedded watermark into the original image by extracting DWT feature from the image. For embedding at Least significant coefficient proposed model has uses Group Search genetic algorithm. Food sources cloning and mutation steps has reduces the iteration count that decreases the embedding process time as well. Experiment was done on real and standard digital images. Result shows that proposed model has maintained the PSNR value of image even after embedding.

Keywords- Data Hiding, Image Processing, Information Embedding, Information Extraction, LSB, MSB.

I. INTRODUCTION

The Internet of Things (IoT) is a term that refers to any forms of linked devices and objects that are connected to the internet, whether wireless or wired. Since these technologies are employed for numerous aims such as transportation, communication, commercial development, and education, the concept's appeal has grown over time. Individuals and organisations can communicate with one other from their remote places thanks to IoT-created hyper-connectivity [1].

With advancements in medical gadget technology, using medical imaging to identify various ailments has become commonplace. Because medical images are transferred through a variety of networks, their security has been a hot concern in recent years. Confidentiality, integrity, and authenticity are all required for the safe transmission of medical pictures. Unauthorized use of such photographs could jeopardise the privacy of patients' information. Furthermore, if these images are susceptible to even little changes, an inaccurate diagnosis might put patients' lives in jeopardy.

With the rapid progress of color photos and the widespread use of sophisticated tools for manipulating digital material, several issues arose, including tampering, modification, forging of digital contents, and violation of intellectual property rights. As a result, copyright material and digital picture integrity are becoming increasingly important security concerns. The use of digital watermarking to secure digital content is common. Watermarking methods are divided into three categories: robust watermarking, semi-fragile watermarking [4], and fragile watermarking [5]. Watermarking technologies that are semi-fragile and fragile are both vulnerable to partial or complete change. The strong watermarking technology, on the other hand, is resistant to common attacks. [6] show that when geometric attacks target watermarked images, removing the watermark is difficult due to translation, scaling, and rotation (TSR). As a result, the most important performance requirements are robustness and imperceptibility.

II. RELATED WORK

The new survey on picture watermarking approaches by **Kumar et al. [12]** was given. SVD can improve imperceptibility, robustness, and reduce false positive effects by using hybrid transform domain approaches. The hybrid approaches were able to improve the extracted watermark's robustness in the face of image processing attacks. The success of hybrid systems, on the other hand, depends on achieving the intended goals using appropriate transform domains.

Pandey et al. [13] proposed incorporating watermark-based DWT-SVD in picture watermarking in their approach. Their method relied on an adjustable embedding strength value derived from perceptual adjustment of the host and watermark picture contents. Their method was able to keep the watermarked image's strength and imperceptibility.

Yadav and Singh [14] proposed image watermarking based on DWT with an adjustable strength factor. Their design offered versatility in terms of its strength factor, which could be altered depending on the image quality. Their scheme was able to withstand a variety of attacks

with ease. As a result, the adaptive scaling factor had a considerable impact on the watermarked image's quality and resilience. The adaptive scaling factor can be used to produce high robustness and invisibility for a variety of picture sources. The goal of this study is to improve robustness while maintaining the quality of the host picture following watermark insertion, which is generated using adaptive embedding strengths.

Ahmadi et al. [15] proposed an image watermarking system based on the DWT-SVD-PSO algorithm. Based on the results of the assaults test and a predetermined objective function, the system used PSO to discover the optimum optimal scaling factors. The PSO is employed to strike a balance between imperceptibility and robustness. Edge entropy and entropy were also employed to choose embedding block locations with increased imperceptibility. On the watermarked image, the scheme achieved good imperceptibility. The system, however, is resistant to attacks such as cropped images, Gaussian filters, and Gaussian noise.

Kang et al. [16] proposed image watermarking using a hybrid of DCT-SVD-DWT with optimal embedding. DWT was used to divide the cover image into four sub-bands. The LL sub-band is broken into eight blocks that do not overlap. The selected eight DCT coefficients are re-arranged into a modulation matrix with two rows and two columns after each block is transformed by DCT. The watermark is embedded by altering the biggest singular values of the matrix, which is generated using SVD.

The recovered watermark was found to be fairly resistant to noise attacks and Gaussian filtering. However, the scheme's imperceptibility performance for an average of eight images yielded a PSNR of 38.63 dB and an SSIM of 0.9662. To put it another way, the technique distorted the quality of the watermarked image significantly.

Taha et al [17] proposed a perceptual mapping model-based adaptive watermarking technique. The perceptual mapping model was created using an integer-based lifting wavelet transform. With an execution time of 1.06 seconds, the technique was able to install a watermark quickly. For fifteen photos, the approach produced less imperceptibility of the watermarked image, with an average PSNR of 36.31 dB and SSIM of 0.96.

III. PROPOSED METHODOLOGY

In this section proposed model was detailed. Input image is pre-process and feature extract for watermark embedding. Fig. 1 shows steps of proposed methodology. Explanation of each block of the fig. 1 is done sequentially. A watermark extraction step was also detailed in the section where fig. 3 is steps of extraction model.

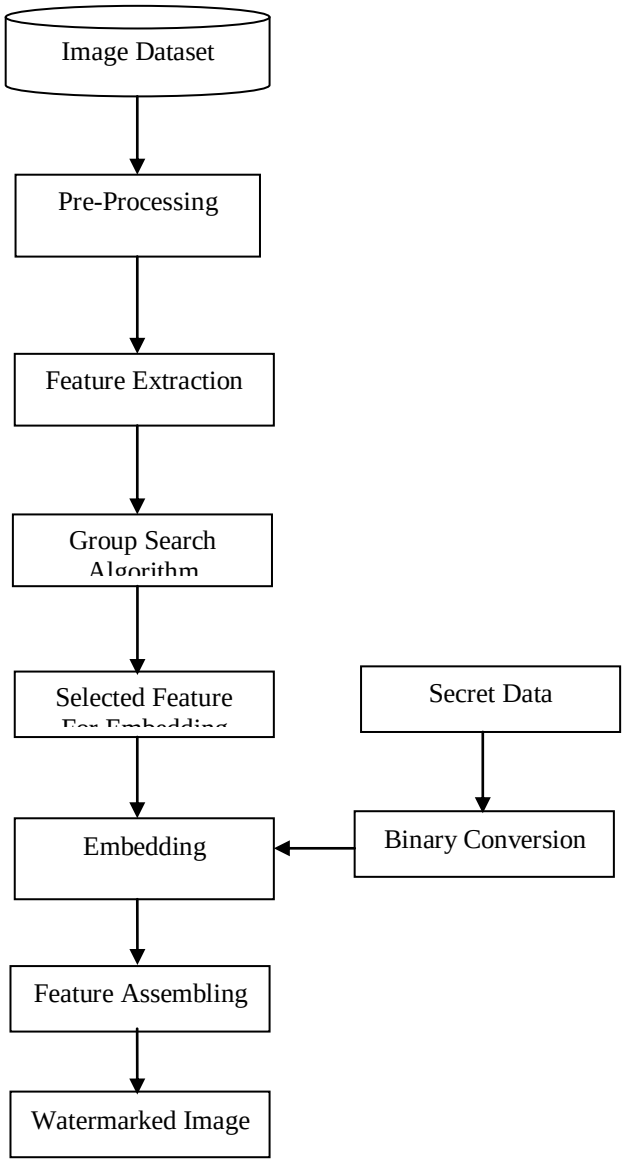


Fig 1. Block diagram of proposed work.

1. Input Image Pre-Processing:
Input image of any dimension is taken as input in the work. This work is compatible with two and three dimension images both. In case of three dimensions matrix (Red) is taken for data hiding. Further image was transform into pixel range of 0 to 255. So if image of HSV format was first transform into RGB format. Let input image is pre-processed as per working environment.

2. Image DWT Feature Extraction:
In this work DWT frequency feature was used. Here DWT feature matrix was used for embedding of watermark in LL region of the image. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain flat region of the image which do not have any edge information, so this is term as approximate version of the image.

3. Group Search Genetic Algorithm:
DWT coefficients obtained from the image was transformed into single dimension matrix. Transformed vector was cluster into set of values one fit for the data hiding and other not fit for data hiding. To cluster vector Group Search genetic algorithm was used in the model.

Group search finds the food to eat where searching member is at any of three state first is producer, second is scrounging and third is ranging. In this work food source is set of binary vectors where 1 represents the feature selection and 0 represents the feature absence. In whole process of Forgaing (Searhcing of food to eat) objective is to finds the good food source.

4. Food Source:
Single dimension vector having two elements. If any element value is change then this new vector is separate food source.

5. Member:
It's a image pixel vaue in the population that points a food source. A member can point different food source at different iteration of algorithm.

6. Group Members:
In this step random set of vector values were select as cluster center in the image. As population has more than one **Food Source**, hence by use of Gaussian random function food sources were generated. Collection of food source is population. In this work two cluster need to be prepare so chromosome is set of two DWT coefficient values.

7. Producing:
As food source values are randomly selected hence evaluation of each food source is required to evaluate. This evaluation was done by fitness function. Euclidian function finds the distance between cluster center value with all other values in the vector. Minimum distance of any value with cluster center value is summed to get the fitness value. Food source having minimum distance sum is consider as best solution.

8. Scrounging:
Population is group into food source subsets. As per the fitness value of each subset food source best chromosome is perform crossover operation with other chromosome in the in the population subset.

Replacement of random cluster value of chromosome with best chromosome cluster value is crossover operation in the work. After crossover operation child food source affinity value decide the updating of population. If child food source affinity is better as compared to any parent food source then poor parent food source is removed from the population otherwise child is not include in the population.

9. Ranging:
In this step random value from the cluster center set of food source is replace by pixel value set of 0 to 255. This operation is done in all food sources of the population.

10. Final solution:
Repeat fitness function and crossover operation of genetic algorithm for T times. After T operations algorithm population fitness value estimate and best fitted food source divide the vector into data hiding values and non hiding values set.

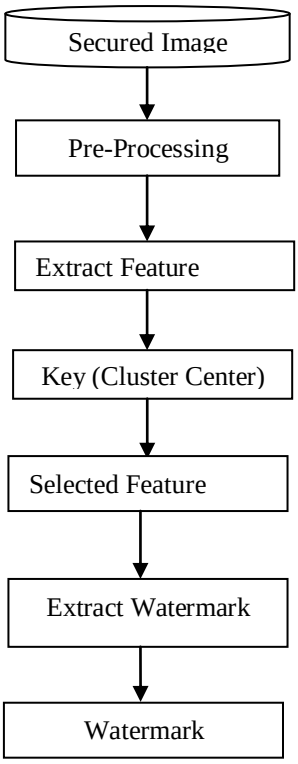


Fig 3. Digital image watermark extraction process block diagram.

11. Data Embedding:
Selected coefficient values were transformed into bits and last three bits were replaced by the model. Once watermark bits are embedded then image is reassembly back into watermarked image.

12. Extraction steps:
In this extraction steps receiver can extract watermark and image by using above block diagram shown in fig. 2. Preprocessing and DWT feature extraction steps are same as done in data hiding step. Further input to the work is Key that is cluster center obtained from the genetic algorithm obtained during embedding process.

As per key coefficient values were cluster into data hiding and non data hiding group. Selected coefficient values were transformed into bits and least significant last three bits were collect to get the watermark from the image.

IV. EXPERIMENT AND RESULTS

This section exhibits the experimental assessment of the proposed procedure for the protection of the picture. All calculations and utility measures were executed by utilizing the MATLAB apparatus. The tests were performed on a 2.27 GHz Intel Core i3 machine, outfitted with 4 GB of RAM, and running under Windows 7 Professional.

1. Dataset:
Analysis done on the standard pictures, for example, mandrilla, lena, tree, and so forth. These are standard pictures which are gotten from http://sipi.usc.edu /database/?volume=misc. Framework is tried on everyday pictures also.

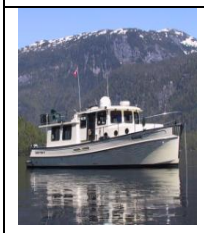
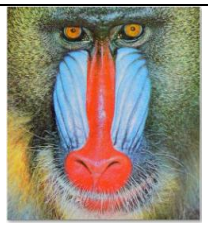
Boat	Baboon	Foreman
		

Fig 4. Dataset Images.

2. Evaluation Parameter:
2.1 Peak Signal to Noise Ratio:
The Peak Signal to Noise Ratio (PSNR) between the images OI and WI which are of size M x N is given by the following expression. Higher is the PSNR, higher is the similarity between the images. It is expressed in dB.

$$\textbf{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

2.2 Signal to Noise Ratio:
Normalized Correlation(NC) The Normalized Correlation (NC) between the images WM and EM which are of size m x n is given by the following expression. Its value ranges in the interval [0 1], closer the NC value to 1 indicates higher is the correlation between the two images.

$$\textbf{SNR} = 10\log_{10}\left(\frac{Signal}{Noise}\right)$$

2.3 Extraction Rate

$$\eta = \frac{n_c}{n_a} \times 100$$

Here n_c is number of pixels which are true.
Here n_a is total number of pixels present in Data Hiding.

2.4 Mean Square Error

$$MSE = \frac{\sum_{i=1}^{n}(X_{obs,i} - X_{model,i})^2}{n}$$

Where X_{obs} are original cover image pixel values and X_{model} was extracted the image. The smaller the means average error, the closer to the ground truth values.

3. Results:

Table 1. Image watermarking PSNR value Based Comparison under ideal condition.

Images	Proposed Model	DWT-DCT coefficients [17]
Boat	55.8099	51.1431
Mandrilla	55.6258	44.8633
House	55.6455	52.8231
Foreman	55.9674	50.0285

Table 2. Image watermarking MSE value Based Comparison under ideal condition.

Images	Proposed Model	DWT-DCT coefficients [17]
Boat	0.1706	0.4998
Mandrilla	0.178	2.122
House	0.1772	0.3394
Foreman	0.1646	0.646

Table 3. Image watermarking NC value Based Comparison under ideal condition.

Images	Proposed Model	DWT-DCT coefficients [17]
Boat	1	0 .95479
Mandrilla	1	0.995
House	1	0.995
Tree	1	0.984
Foreman	1	1

Table 1, 2 and 3 shows that proposed model has maintain the image quality after embedding of watermark. It was obtained that use of group search genetic algorithm for embedding of watermark bit in selected coefficient of DWT region has increase the embedding quality.

Table 4. Image watermarking PSNR value Based Comparison under noise attack.

Images	Proposed Model	DWT-DCT Coefficients [17]
Boat	7.2239	5.8194
Mandrilla	7.86	5.7991
House	7.3033	6.3396
Foreman	5.5224	3.4238

Table 5. Image watermarking MSE value Based Comparison under noise attack.

Images	PROPOSED MODEL	DWT-DCT Coefficients [17]
Boat	1232.2	17027
Mandrilla	10640	17107
House	12099	15105
Tree	1513.8	21949
Foreman	18232	29560

Table 5, 6 and 7 shows different attack parameter values of both comparing watermarking models. This paper has shown that in ideal and attack environment proposed model is better in all condition. This attack condition on different image set has shown that proposed work has efficiently improved the secret message extraction percentage in all testing sets.

V. CONCLUSIONS

Digital world has change the lifestyle of people and improved the ease of working in various field of technical and non-technical area. This digital communication need authentication that data is valid and generate from the verified sender. This paper has proposed a model that extract DWT feature from the image for secret data embedding.

Selection of embedding block is done by Group Search Optimization genetic algorithm that partly selects image area for embedding and partly image blocks are rejected. Experimental work has shown in real image dataset and result shows that proposed model has improved all set of evaluation parameter values. It was found that average improvement in PSNR value in all set of digital image dataset. In future scholar can improve embedding work by further enhancing the feature set.

REFERENCES

[1] J. Porras, J. Pänkäläinen, A. Knutas, and J. Khakurel, ‘‘January security in the Internet of Things—A systematic mapping study,’’ in Proc. 51st Hawaii Int. Conf. Syst. Sci., 2018, pp. 3750–3759.

[2] F. Alsubaei, A. Abuhussein, and S. Shiva, ‘‘Security and privacy in the Internet of medical things: Taxonomy and risk assessment,’’ in Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops), Oct. 2017, pp. 112–120.

[3] M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, ‘‘Secure medical data transmission model for IoT-based healthcare systems,’’ IEEE Access, vol. 6, pp. 20596–20608, 2018.

[4] M. K. Hasan, A. F. Ismail, S. Islam, W. Hashim, M. M. Ahmed, and I. Memon, ‘‘A novel HGBBDSA-CTI approach for subcarrier allocation in heterogeneous network,’’ Telecommun. Syst., vol. 70, no. 2, pp. 245–262, Feb. 2019

[5] D.-C. Wu and W.-H. Tsai, ‘‘A steganographic method for images by pixel-value differencing,’’ Pattern Recognit. Lett., vol. 24, pp. 1613–1626, Jun. 2003.

[6] C.-C. Chang and H.-W. Tseng, ‘‘A steganographic method for digital images using side match,’’ Pattern Recognit. Lett., vol. 25, no. 12, pp. 1431–1437, Sep. 2004.

[7] A. Sahu, G. Swain, M. Sahu, and J. Hemalatha, ‘‘Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP,’’ Journal of Information Security and Applications, 58, Apr. 2014, Art. no. 102808.

[8] A. Sahu and G. Swain, ‘‘An optimal information hiding approach based on pixel value differencing and modulus function,’’ Wireless Pers. Commun., vol. 108, no. 1, pp. 159–174, 2019.

[9] C.-C. Chang, W.-L. Tai, and K.-N. Chen, ‘‘Improvements of EMD embedding for large payloads,’’ in Proc. 3rd Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP), Nov. 2007, pp. 473–476.

[10] C.-C. Chang, Y.-C. Chou, and T. D. Kieu, ‘‘An information hiding scheme using sudoku,’’ in Proc. 3rd Int. Conf. Innov. Comput. Inf. Control, 2008, p. 17.

[11] C. C. Chang, Y. Liu, and T. S. Nguyen, ‘‘A novel turtle shell based scheme for data hiding,’’ in Proc. 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process., Aug. 2014, pp. 89–93.

[12] C. Kumar, A. K. Singh, and P. Kumar, ‘‘A recent survey on image watermarking techniques and its application in e-governance,’’ Multimedia Tools Appl., vol. 77, no. 3, pp. 3597–3622, Feb. 2018.

[13] P. Pandey, S. Kumar, and S. K. Singh, ‘‘Rightful ownership through image adaptive DWT-SVD watermarking algorithm and perceptual tweaking,’’ Multimedia Tools Appl., vol. 72, no. 1, pp. 723–748, Sep. 2014.

[14] N. Yadav and K. Singh, ‘‘Robust image-adaptive watermarking using an adjustable dynamic strength factor,’’ Signal, Image Video Process., vol. 9, no. 7, pp. 1531–1542, Oct. 2015.

[15] S. B. B. Ahmadi, G. Zhang, S. Wei, and L. Boukela, ‘‘An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics,’’ Vis. Comput., vol. 35, pp. 385–409, Feb. 2020.

[16] X.-B. Kang, F. Zhao, G.-F. Lin, and Y.-J. Chen, ‘‘A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength,’’ Multimedia Tools Appl., vol. 77, no. 11, pp. 13197–13224, Jun. 2018.

[17] T. B. Taha, R. Ngadiran, and P. Ehkan, ‘‘Adaptive image watermarking algorithm based on an efficient perceptual mapping model,’’ IEEE Access, vol. 6, pp.

66254–66267, 2018.

[18] Qingtang Su, Decheng Liu, Zihan Yuan, Gang Wang, Xiaofeng Zhang, Beijing Chen, And Tao Yao. "New Rapid and Robust Color Image Watermarking Technique in Spatial Domain". IEEE Access March 25, 2019. http://sipi.usc.edu/database/?volume=misc.