Vinay Kumar Shukla, 2023, 11:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Environmental Image Watermarking Using Butterfly Genetic Algorithm (EIWBA)

Vinay Kumar Shukla, Prof. Manish Gurjar
Department of Electronics & Communication Engineering
Technocrats Institute of Technology - Advance, Bhopal
Madhya Pradesh, India

Abstract: Environmental images taken from the satellite were used for the analysis of different type of forecasting, like weather, crop yield, etc. In order to provide the authenticity of the valid source watermark embedding is need to be done. This work has proposed a model Environmental Image Watermarking using Butterfly algorithm (EIWBA) that embedded watermark into the environmental image. For selection of embedding pixel values butterfly genetic algorithm was used. Selected region for embedding by butterfly algorithm increases his robustness of the image against noise attack. Experiment was done on real dataset images and result shows that proposed model has improved the work performance.

Keywords: Data Hiding, Image Processing, Information Embedding, Information Extraction.

I. INTRODUCTION

The development of technologies makes it possible to represent the world around us and save it in a certain digital form, such as image, audio, video, and text [1]. Digital media has become an inseparable part of our daily life, which makes it convenient to record activities, express and share emotions with each other. The easy-to-use technologies, allow non-professional users to manipulate the multimedia data easily, such as the editing tool PhotoShop [2]. On the one side, with the perspective of information hiding, much more information can be embedded within the image purposely. Some of these services are social network, online market. But these technologies give rise to new problem of piracy or in other words proprietary get easily stolen. So to overcome these different techniques are used for preserving the proprietary of the owner. Invisible digital watermarking is one of approach to provide privacy of the proprietorship, this is sub-branch of the information hiding where watermark is considering as the hiding information while original information is considering as the carrier like photographs, digital music, or digital video [1, 2, 4]. One of the basic causes of the copyright issue is the ease available of the internet and some software that can modify the content as per the user requirement.

Electronic document security was and continues to be one of the most pressing issues in scientific research. Intruders are unlawfully reproducing, authenticating, and disseminating digital materials as Internet capabilities advance. [3] As a result, watermarking technologies were researched for many applications, like transmitting, monitoring, intellectual property rights, document validation, and copying limitation. Copyright violations, unauthorized usage, replication, and online media theft became more common as a result of the widespread uploading and dissemination of electronic material on the Internet.

The digital media nowadays that usually has higher resolution needs a huge memory space to store. The fact, however, is that there are amounts of redundancy in the digital media, which can be removed for time-saving. Meanwhile, it offers an opportunity to hide information by modifying the image information directly [3].

II. RELATED WORK

In [7], robust Elliptic curve based image encryption and authentication model for both grayscale and color images has been proposed. The model uses the secure Elliptic Curve Dife- Hellman (ECDH) key exchange to compute a shared session key along with the improved ElGamal encoding scheme. 3D and 4D Arnold Cat maps are used to effectively scramble and transform the values of plain image pixels. A well-structured digital signature is used to verify the authenticity of the encrypted image prior to decryption.

In [8], authors address the security level concern of an image encryption technique combining ECC with Hill cipher (ECCHC) which has been recently proposed by Dawahdeh et al [9]. Our study rises concern about some weaknesses and flaws of the analyzed encryption scheme against some plain-text and known plain-text attacks. In addition, and not least issue, it is found that the key length used in Dawahdeh et al. scheme is not sufficiently large to be robust against brute force attack. To fix the found flaws and to improve the encryption scheme, a generalized cryptosystem is suggested.

In [10], after generating a unique key using random characters the plain text is encrypted into ciphertext. To do this encryption, a divide and circular left and right shift approach is followed, and conversely, the reverse is maintained for decryptions as well.

In [11] authors, presents an intelligent symmetric cryptography with a chaotic map and quantum-based key generator (KG) for medical image encryption and decryption. Overall scheme processes include (1) random cipher code generation, (2) training gray relational analysis (GRA)-based encryptor and decryptor, and (3) decrypted image evaluation. The hybrid chaotic map and quantum-based KG are used to increase the chaotic complexity and unpredictable levels to produce cipher codes for changing pixel values (substitution method) in a 2D image by 256 key-space cipher codes. The first and second GRA models are used to train the cipher codes to achieve an encryptor and a decryptor, respectively. Through the methodology validation using a chest X-ray database, the structural similarity index measurement is employed to evaluate the decryption quality between the plain image and decrypted image.

In [14] authors perform the cryptanalysis of a newly proposed color image encryption scheme using RT-enhanced chaotic tent map (CTM). By using chosen-plaintext attacks, the equivalent keys of the cryptosystem are successfully broken, so that the target ciphertext image can be decoded. Based on the cryptanalysis, we then proposed an improved encryption algorithm. A new Logistic-tent map (LTM) is proposed and applied to the improved encryption algorithm, and a parameter related to the SHA-3 hash value of the plaintext image is introduced as a secret key parameter so that the improved algorithm can resist chosen-plaintext attacks.

In [15] quantum steganography approach is proposed to hide a quantum secret image into a quantum cover image. The quantum secret image is encrypted first using a controlled- "NOT" gate to demonstrate the security of the embedded data. The encrypted secret image is embedded into the quantum cover image using the two most and least significant qubits. In addition, a quantum image watermarking approach is presented to hide a quantum watermark gray image into a quantum carrier image. The quantum watermark image, which is scrambled by utilizing Arnold's cat map, is then embedded into the quantum carrier image using the two least and most significant qubits. Only the watermarked image and the key are sufficient to extract the embedded quantum watermark image. The proposed novelty has been illustrated using a scenario of sharing medical imagery between two remote hospitals.

Sahu et al. [17] utilized multi-directional block-based PVD as well as modulus function resisting PDH and RS-steganalysis. Sahu and Swain [18] developed the best information concealing solution possible by using the PVD method and the modulus function as their foundation. techniques that are state-of-the-art in both digital image steganography and steganography analysis.

II. PROPOSED METHODOLOGY

In this section proposed model Environmental Image Watermarking using Butterfly algorithm (EIWBA) was detailed. Input image is pre-process and color feature extract for watermark embedding. Fig. 1 shows steps of proposed methodology. Explanation of each block of the fig. 1 is done sequentially. Watermark extraction steps was also detailed in the section where fig. 2 is steps of extraction model.

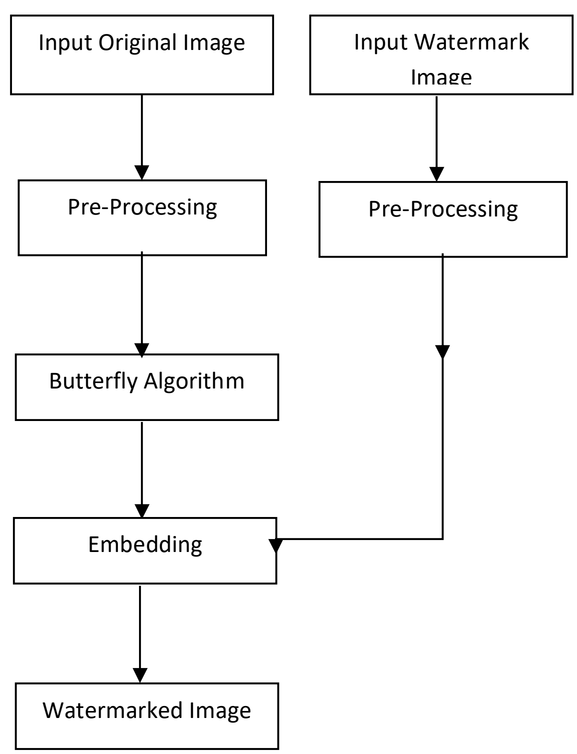


Fig.1 Block diagram of EIWBA work.

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-dimension 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. In this work color feature was used.

Butterfly Algorithm
Generate Population: At this step, different sets of chromosomes were made, each with a number between 0 and 255. So each image set is like a gene or a butterfly (BP), and all of them together are called the population (P). This can assume as let BP = [b_1, b_2, ….b_m] as the chromosome set where m is number of butterfly in population. where b = [P_1, P_2,…P_n] n is number of cluster to be obtain.

BP ←Generate_Butterfly (n, m) --------- (1)

Fitness Function
As butterfly values are chosen at random, fitness value estimate is used to judge each one. The Euclidian function finds the distance between the center values of a cluster and all the other values in the vector. The fitness value is the minimum distance of any value from the cluster center value. The best option is the butterfly whose distances add up to the least.

$$Bfit_m \leftarrow \sum_1^x \sum_1^y Min(I_{x,y} - BP_m) \text{--------- (2)}$$

Evaluate L-Best and G-Best
This step finds the best butterfly from the population, and the fitness value of this best answer acts as both the local best and the global best. In this case, it was found by figuring out how fit each possible answer in the group was. After this step, the program moves on to the next step, where L-Best and G-Best are regularly updated.

$$L_{best} \leftarrow Min(Bfit)$$

Iteration Steps This involve calculation of Sensitivity of Butterfly by eq. 3 than cognitive values with constriction factor and inertia weight were evaluate by eq. 6, 7. Here velocity and position of the butterfly also get update which are parameters of PSO. So as per position matrix crossover is done to update population.

Sensitivity of Butterfly

$$S = e^{-(M_r - C_r)/M_r} \text{---- 3}$$

Where S is sensitivity of r^{th} iteration where M_r is maximum number of iteration takes place and Cr is current iteration of this BF-PSO algorithm.

Cognitive and Social parameters

$$C_1 = y * \left(\frac{C_r}{M_r} + x\right) \text{---------------4}$$

$$C_2 = x * \left(\frac{C_r}{M_r}\right) \text{--------------5}$$

Where x, y are constants
Constriction Factor C_{eq}

$$\alpha = C_1 + C_2$$

$$C_{eq} = 1 - \alpha - \sqrt{\alpha^2 - 4\alpha} \text{---- 6}$$

Intertia Weight W

$$W = y + \frac{(M_r - C_r)}{M_r} \text{----- 7}$$

Update velocity V and position X

$$V_{i+1} = C_{eq} * (W * V_i + S \quad * (1 - P) * R * C_1 * (L_{best} - C_r) + P * R' * C_2 * (G_{best} - C_r) \text{-------------8}$$

$$X = R*P*V_{i+1} \text{-----9}$$

In above equation V is velocity, X is position while R and R' are random number whose values change between 0-1. p is probability of nectar for the butterfly selection. So as per X and V values crossover operation were performed.

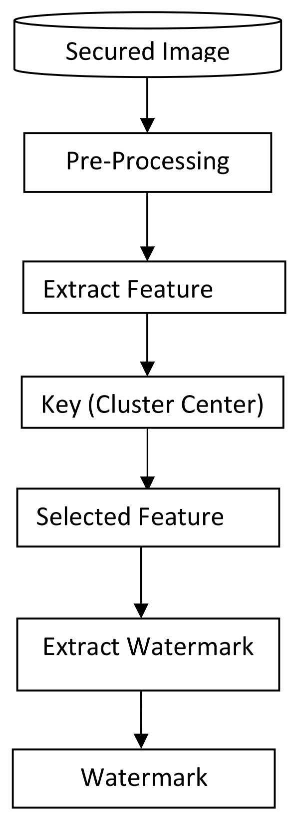


Fig.2 Digital image watermark extraction process block diagram.

Crossover
In this work, the population P is changed based on X columns, and P is changed based on V rows. If you change something in a column, it helps you find a new place for the cluster center in the same likely answer. While changes to the row values based on the Lbest answer make it more likely that a better fitness will be made.

Update G-Best
After each cycle, the G-Best values are optimized if the values of the new solution's likely solution fitness function are better than the values of the old G-Best. So, iteration will break if two iterations show the same numbers.

Final solution: To get the final solution run the genetic algorithm's fitness function and crossover process T times. After T processes, the method estimates the fitness value of the population and finds the best-fitting chromosome. It then splits the vector into sets of data hiding values and non-hiding values.

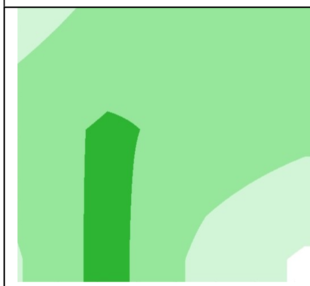
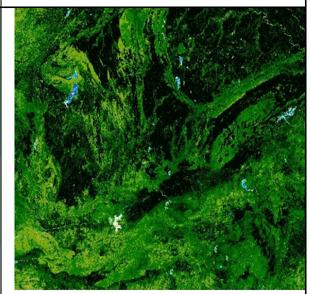
Data Embedding
Selected region by butterfly pixel values were turned into bits, and the model replaced the last three bits. Once the watermark bits are added, the picture is put back together to make a watermarked image.

Extraction steps
Fig. 2 shows a block diagram that can be used in this step to extract the watermark from the image. The steps of preprocessing and getting color features are the same as those in the step of em data. Key, which is the butterfly cluster center output and was found by the genetic algorithm during the embedding process, is another thing that goes into the work. Based on the key pixel values, the groups were split into those that hide data and those that don't. Some pixel values were turned into bits, and the least important last three bits were used to get the image's stamp.

IV. EXPERIMENT & RESULTS

This section of paper shows how the proposed method for protecting the picture was tested in the real world. The MATLAB tool was used to do all the math and energy measurements. The tests were done on a computer with a 2.27 GHz Intel Core i3 processor, 4 GB of RAM, and Windows 7 Professional.

Dataset
Experiment is done on real dataset having values of the SPI from https://iridl.ldeo.columbia.edu/maproom/Global/Precipitation/SPI.html. While NDVI value obtained from http://iridl.ldeo.columbia.edu/SOURCES.

SPI	NDVI
	

Results

Table 1. PSNR value based Environmental image watermarking model comparison.

Images	EIWBA	**DWT-DCT coefficients [17]**
SPI-1	58.1678	50.6906
SPI-2	59.7753	49.9544
SPI-3	58.5333	50.1167
NDVI-1	58.5577	48.6379
NDVI-2	52.7516	44.3811
NDVI-3	52.4003	50.3412

Table 1 shows that proposed EIWBA model has increases the work performance by the use of butterfly genetic algorithm. It was found that in both type of environmental images performance average PSNR value was improved by 13.54% as compared to previous model.

Table 2 MSE value based Environmental image watermarking model comparison.

Images	EIWBA	**DWT-DCT coefficients [17]**
SPI-1	0.0992	0.5546
SPI-2	0.0685	0.657
SPI-3	0.0911	0.633
NDVI-1	0.0906	0.8898
NDVI-2	0.3451	2.3712
NDVI-3	0.3742	1.0092

Mean square error values of the watermarking models were shown in table 2. As embedding was done in selected pixel position specified by butterfly algorithm has reduces the work MSE value 4.72%, as compared to []. This reduction is just because of placement of LSB bits by watermark.

Table 3. NC value based Environmental image watermarking model comparison.

Images	EIWBA	DWT-DCT coefficients [17]
SPI-1	1	1
SPI-2	1	1
SPI-3	1	1
NDVI-1	1	0.879
NDVI-2	1	0.916
NDVI-3	1	0.939

Table 3 shows the normalized correlation parameters value of watermarking algorithm; it was found that in case of SPI image set results were 1 in both comparing models. But in case of NDVI images previous model not fully recover watermark image from the embedded images. It was found that proposed EIWBA has improved the NC value by 4.43% as compared to previous work.

Table 4 PSNR value based Environmental image watermarking model comparison, under noise attack.

Images	EIWBA	DWT-DCT Coefficients [17]
SPI-1	1.2402	1.2344
SPI-2	0.5174	0.5123
SPI-3	0.6836	0.6784
NDVI-1	11.3667	11.4151
NDVI-2	5.6128	5.6193
NDVI-3	6.2083	6.2138

Table 5. MSE value based Environmental image watermarking model comparison, under noise attack.

Images	EIWBA	DWT-DCT Coefficients [17]
SPI-1	4.8871	4.8937
SPI-2	5.7722	5.7789
SPI-3	5.5555	5.5622
NDVI-1	4.7469	4.6942
NDVI-2	1.7857	1.7830
NDVI-3	1.5569	1.5549

Table 3. NC value based Environmental image watermarking model comparison, under noise attack.

Images	EIWBA	DWT-DCT coefficients [17]
SPI-1	0.663	0.661
SPI-2	0.645	0.664
SPI-3	0.669	0.65
NDVI-1	0.872	0.784
NDVI-2	0.5098	0.477
NDVI-3	0.681	0.673

Experimental values of noise attacks were shown in table 4, 5 and 6. It was found that PSNR and NC values was high in all set of SPI, NDVI images. Further it was found that proposed model has increase the work performance by the MSE value was also reduces the EIWA watermarking model.

VI. CONCLUSION

This paper has proposed an image watermarking model by using genetic algorithm. Butterfly genetic algorithm was used for the selection of color feature position for embedding of watermark into two regions. Experiment was done on real environmental images taken from valid sources. Result shows that proposed EIWBA model has increases the work performance by the use of butterfly genetic algorithm. It was found that in both type of environmental images performance average PSNR value was improved by 13.54% as compared to previous model.

REFERENCES

1. Key Dependent Image Steganography Using Edge Detection Shahzad Alam, Vipin Kumar, Waseem A Siddiqui and Musheer Ahmad. 2014 Fourth International Conference on Advanced Computing & Communication Technologies.
2. Tamanna Tabassum, S.M. Mohidul Islam "A Digital Image Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT" vol. 13, no. 7, pp. 560 –576, july 2003.
3. Frank Hartung, Jonathan K. Su, and Bernd Girod "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks". of Multimedia Contents" International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.
4. "Chapter 2. Wavelet Transforms On Images" *sundoc.bibliothek.uni-halle.de/diss-online/02/03H033/t4.pdf*
5. Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, Ankita Tawde Digital Video Watermarking Using Modified LSB And DCT Technique. International Journal of Research in Engineering and Technology eISSN: 2319-1163.
6. P. Parida, C. Pradhan, X. -Z. Gao, D. S. Roy and R. K. Barik, "Image Encryption and Authentication with Elliptic Curve Cryptography and Multidimensional Chaotic Maps," in IEEE Access, vol. 9, 2021.
7. Mustapha Benssalah, Yesser Rhaskali, Karim Drouiche. "An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography". Multimedia Tools and Applications 2021.
8. Dawahdeh ZE, Yaakob SN, bin Othman RR. "A new image encryption technique combining elliptic curve cryptosystem with Hill Cipher". Journal of King Saud University-Computer and Information Sciences 30(3): 2018.
9. K. I. Masud, M. R. Hasan, M. M. Hoque, U. D. Nath and M. O. Rahman, "A New Approach of Cryptography for Data Encryption and Decryption," 2022 5th International Conference on Computing and Informatics (ICCI), 2022.
10. C. -H. Lin et al., "Intelligent Symmetric Cryptography with Chaotic Map and Quantum Based Key Generator for Medical Images Infosecurity," in IEEE Access, vol. 9, pp. 118624-118639, 2021.
11. Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, And Xiaojie Guo. "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation". IEEE Transactions On Cybernetics 2015.
12. Mohammed A. M. Abdullah, Satnam S. Dlay, Wai L. Woo Jonathon A. Chambers. "A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography"., IEEE Access, 2016.
13. Congxu Zhu, And Kehui Sun. "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps". IEEE Access VOLUME 6, 2018.
14. Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, M. Shamim Hossain, Md. Abdur Rahman, Atif Alamri, B. B. Gupta. "Efficient quantum information hiding for remote medical image sharing". IEEE ACCESS, 2017.
15. Donghui Hu, Dan Zhao, Shuli Zheng. "A New Robust Approach for Reversible Database Watermarking With Distortion Control". IEEE Transactions On Knowledge and Data Engineering, 2019.
16. 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.