ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.7, 4533–4541
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.7.22 Spec. Issue on RDESTM-2020

A SECURED IMAGE STEGANOGRAPHY USING GENETIC ALGORITHM

SABYASACHI PRAMANIK[1] AND S. SURESH RAJA

ABSTRACT. According to the optimization techniques examined in the past, the performance of Genetic Algorithm (GA) based approaches are seen as a substandard technique compared to PSO based approaches with a target to improve the performance of GA approach. The modification in GA is performed and proposed in this work. The modification performed in the GA based methodologies is modification in the hybrid operator. These GA are applied with Fresnelet Transform (FT) and Discrete Ripplet Transform (DRT). The experimental outcomes have tried the efficiency of the proposed work as far as the performance measures are concerned. The GA explores the wellness surface by this hybrid strategy. The best two wellness people are chosen to deliver new offsprings. The last two low wellness people are disposed of and they leave a space for two new posterity in the following iteration. In this paper, the process of hybrid operation from the parent people is clarified.

1. INTRODUCTION

Steganography [1] is the specialty of concealing data in a spread media for secret and secure [2] correspondence. The acquired picture which conveys the secret data or data is named as stego picture. The presence of secret data in the stego picture can't be distinguishable to any unplanned individual. The significant characteristics of any steganographic framework are (i) high limit payload installing (ii) better PSNR (iii) power to some mutilation brought about

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68U10, 68W50.

Key words and phrases. Genetic Algorithm, Steganography, QR-code.

by un approved people or clamors in the correspondence frameworks. The prerequisites of Steganographic frameworks are implanting module and recovery module. The inserting module at the sender's end capacitates in implanting the secret data or payload to the spread picture to get stego picture utilizing any one of the steganographic strategies.

The recuperation module at the gatherer's end applies inverse steganographic technique figuring to expel the covered secret data from the stego picture. The utilization of steganography can be utilized to guarantee ensured development rights i.e., to maintain copyright and moreover to pass on data to simply those components who are endorsed.

Steganography gives an approach to convey secretly up to an aggressor who doesn't figure out how to recognize the message. The most reasonable kinds of documents for steganographic transmission are media records because of their huge size. The host records hiding different documents are generally called bearers. The transporter records are practical documents and does not bring up an issue or excite doubt. This area records various concealing methods that are being ultimately utilized. Data can be installed inside a record by exploiting human discernment. Sound documents use recurrence veiling on tones with comparative frequencies and the easygoing audience does not hear the covered calmer tone.

1.1. **Steganography Techniques.**

Video. Video steganography [3] is a blend of sound and image procedures. The video documents normally have separate inward records for picture and sound. Steganography procedures can be connected to video and sound. The insignificant size of any video document shows the degree for concealing a lot of secret data but then goes undetected.

DNA. Data stowing away is done in DNA strands as clarified by Peterson. DNA strands are comprised of bases like adenine (A), thymine (T), cytosine (C) and guanine (G), which distend from a sugar-phosphate spine. Arrangement is drawn speaking to three base mixes. To make a secret message, DNA is combined utilizing this arrangement of bases. Secret data is put between DNA strands and go about as markers for secret communication. DNA strands are

added haphazardly to avoid the identification of the secret message. DNA's being moment like speck is sent in a volume, along these lines making it hard to follow and recover.

1.2. **Issues in Steganography.** Steganography issues are explicit in its area. A typical peril in steganography is covering up malware [4], spyware [5], infection or Trojans [6] in pictures of email connections. The least difficult approach to hide malware is utilizing twofold expansions. Microsoft Windows hides the last piece of record augmentations. A record with twofold expansion like AnnaKournikova.jpg.vbs is appeared as an image document, neglected and after that executed. Inserted Macros in Microsoft word execute on open record and automatically duplicate utilizing the email locations put away in a location book like the Melissa infection. Infection or Trojan can be customized to hide significant documents in a computer and unhide them for a payment like a variation of the Melissa infection. Contentions keep on seething among government and people, primarily because of the distributing and broadcasting industry enthusiasm for concealing copyright, sequential numbers and interactive media documents. Current choices for cryptographic [7] choices are restricted and the accessibility of open encryption can be put. In spite of the fact that solid encryption techniques are accessible to the overall population, it is additionally a danger to open security and wellbeing, since it very well may be put to wrong use by crooks. Steganography can be utilized by psychological militants and lawbreakers for their communication as steganographic trades have restricted recognizability.

2. METHODOLOGY

In the initial step, the specific transform is applied on the spread image to get the host image. In the following stage, the mystery information have image and the comparing chromosome is set up to accomplish the pixel bits utilizing the chromosome qualities. A short time later, the mystery information is changed over to the Quick Response (QR) code [8] bit groupings depending on the mystery information direction of the chromosome quality (for example QR-Dir). At that point, the quantity of host pixel bits and QR code pixel bits are thought about. In the event that the quantity of QR code bits is more than the host pixel

bits, there won't be the option to embed the mystery bits in a host image. Else, we will have the option to embed in the comparing host bits. In the wake of embeddings in the mystery information, the stego image is acquired by applying backwards specific transform and afterward fitness worth is determined. In GA, let the all out number of individual is 15; in this way for 15 individuals, 15 fitness esteem (PSNR) [9] is created.

The secret information is extracted by applying the specific transform to the stego image. At that point, the utilized chromosome is extracted from the predefined pixel bits and isolates its comparing qualities. The pixel bit sequence is acquired from the chromosome qualities. From this, the first QR code mystery information bits sequence is acquired. The last sequence of mystery bits is accomplished at long last depending on the chromosome qualities which produce the QR code mystery image in a similar manner. At that point, the reverse specific transform is applied to get the first spread image.

The image steganography utilizing Fresnelet Transform [10] and modified Genetic Algorithm (GA) [11] is performed. The hugest Fresnelet Transform coefficients [12] are chosen with modified GA to insert the QR coded [13] mystery image. The resultant stego images appear as in Figure 1. The performance measures of consolidated FT and modified GA on stego image appear as in Table 1.

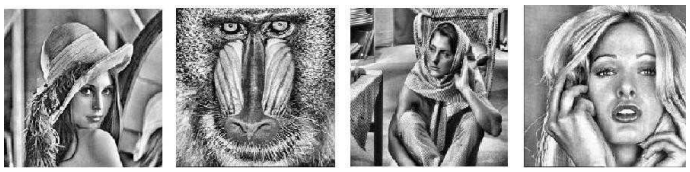
TABLE 1. Scanning Order 1 and 2

25	24	23	22	21
20	19	18	17	16
15	14	13	12	11
10	9	8	7	6
5	4	3	2	1

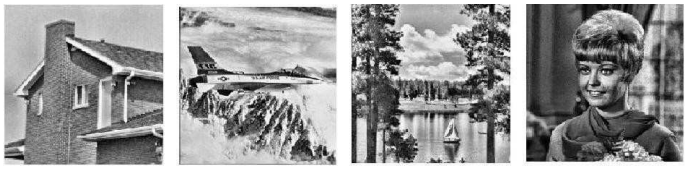
25	20	11	10	5
24	19	12	9	4
23	18	13	8	3
22	17	14	7	2
21	16	15	6	1

In this test, the image steganography utilizing Fresnelet Transform and modified GA is performed. The hugest FT coefficients are chosen with modified GA to insert the QR coded mystery image.

A normal PSNR estimation of 50.28 has been accomplished by the proposed technique. Essentially, the normal estimation of installing capacity is 139389 bits which shows that the huge measure of information can be inserted in the spread image.



(a) (b) (c) (d)



(e) (f) (g) (h)

FIGURE 1. Stego images using combined FT and modified GA: (a) Lena (b) Baboon (c) Barbara (d) Tiffany (e) House (f) Plane (g) Sail boat (h) Girl

3. RESULT

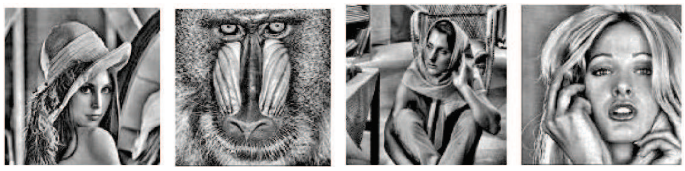
The image steganography utilizing Discrete Ripplet Transform and modified GA is performed. The cover image is partitioned into little squares and DRT is applied to each square to acquire the ripplet coefficients. The best DRT coefficients are chosen with modified GA. The information is covered up in those best coefficients. At long last, the converse DRT is performed to acquire the stego image. The performance measures of joined DRT and modified GA on stego image appear as in Table 2. CC and SSIM indicate the Correlation Coefficients [14] and Structural Similarity Index [15] respectively.

The restored cover image and QR coded mystery message after extraction appear in Figure 2 and 3. The performance measures of joined DRT and modified GA after extraction appear as in Table 3.

From Table 3, an average Tamper Assessment Function (TAF) [16] value of 0.01 and Normalized Absolute Error (NAE) [17] value of 0.003 is achieved with the proposed method.

TABLE 2. Performance measures of combined DRT and modified GA based data embedding

Images	PSNR (dB)	Embedding Capacity (bits)	CC	SSIM	Embedding Time (seconds)
Lena	50.57	157761	1.0000	0.9999	673
Baboon	50.36	157774	1.0000	0.9999	663
Barbara	50.39	157761	1.0000	0.9999	691
Tiffany	50.54	157772	1.0000	0.9999	606
House	50.47	157746	1.0000	0.9999	620
Plane	50.59	157769	1.0000	0.9999	629
Sail boat	50.46	157766	1.0000	0.9999	754
Girl	50.39	157750	1.0000	0.9999	753
Average Value	50.47	157762	1.0000	0.9999	674



(a) (b) (c) (d)

(e) (f) (g) (h)

FIGURE 2. Restored cover images using combined DRT and modified GA: (a) Lena (b) Baboon (c) Barbara (d) Tiffany (e) House (f) Plane (g) Sail boat (h) Girl

CONCLUSION

GA has been modified to improve the stego image quality and installing capacity. FT and DRT transforms are utilized in this work. Methodological clarification as for the proposed calculations is examined in this section. The inquiry

TABLE 3. Performance measures of combined DRT and modified GA based data extraction

Images	Tamper Assessment Factor (TAF)	Normalized Absolute Error (NAE)	Extraction Time (seconds)
Lena	0.01	0.004	629
Baboon	0.01	0.003	641
Barbara	0.01	0.004	733
Tiffany	0.01	0.002	617
House	0.01	0.002	563
Plane	0.01	0.004	546
Sail boat	0.01	0.004	581
Girl	0.01	0.004	620
Average Value	0.01	0.003	616

FIGURE 3. Restored QR coded Secret data using combined DRT and modified GA

and optimization problem in steganography frameworks has been unraveled by utilizing GA. The primary preferred position of the proposed modified GA based steganography framework is that it maintains a strategic distance from the debilitating looking through problem in steganography; it upgrades the subtlety and accomplishes high inserting capacity contrasted with the past techniques. Further it keeps up the time utilization to run the program. It is apparent from the performance measures of the proposed calculation that the Discrete Ripplet Transform can beat the Fresnelet Transform.

REFERENCES

[1] W. ABDUALLAH: *A Review on Steganography Techniques*, American Scientific Research Journal for Engineering, Technology and Sciences, **24**(1) (2016) 131–150.

[2] S. PRAMANIK, R.P. SINGH, R. GHOSH: *A New Encrypted Method in Image Steganography*, Indonesian Journal of Electrical Engineering and Computer Science, **14**(3) (2019), 1412–1419.

[3] B. CHANDEL, S. JAIN: *Video Steganography: A Survey*, IOSR Journal of Computer Engineering, **18**(1) (2016), 11–17.

[4] S. WISEMAN: *Stegware–Using Steganography for Malicious Purposes*, doi: 10.13140/RG.2.2.15283.53289.

[5] BASAHEL, A. M., YAMIN, M., SEN, A.: *Enhancing Security of Transmitted Data by Improved Steganography Method*, vol. 19, no. 4, 239–244.

[6] S. ABARCA: *An Analysis of Network Steganographic Malware*, Master thesis, 10.13140/RG.2.2.33593.62564.

[7] S. PRAMANIK, S.K. BANDYOPADHYAY: *Application of Steganography in Symmetric Key Cryptography with Genetic Algorithm*, International Journal of Computers and Technology, **10**(7), 1791–1799.

[8] G. PRABAKARAN: *QR-code Image Steganography*, doi: 10.13140/RG.2.1.1296.9848.

[9] S. PRAMANIK, S.K. BANDYOPADHYAY: *Hiding Secret Message in an Image*, International Journal of Innovative Science, Engineering and Technology, **1**(3), 553–559.

[10] N. MUHAMMAD, N. BIBI, M.Z. ZAHID, D.G. KIM: *Blind Data Hiding Technique using the Fresnelet Transform*, Springer Plus, **4**(832) (2015), DOI 10.1186/s40064-015-1534-1.

[11] S. PRAMANIK, R.P. SINGH, R. GHOSH: *Application of Bi-orthogonal Wavelet Transform and Genetic Algorithm in Image Steganography*, Multimedia Tools and Applications, **79** (2020), 17463–17482. https://doi.org/10.1007/s11042-020-08676-1.

[12] S.D. MAHESWARI, JUDE: *Frequency domain QR code based image steganography using Fresnelet transform*, AEU - International Journal of Electronics and Communications. **69**(2) (2015), 539–544, DOI:10.1016/j.aeue.2014.11.004.

[13] V. HAJDUK, M. BRODA, O. KOVAC, D. LEVICKY: *Image Steganography with using QR code and cryptography*, 26th IEEE Conference Radioelekronika, Kosice 2016, pp. 350-353, doi: 10.1109/RADIOELEK.2016.7477370.

[14] R. REJANI, D. MURUGAN, D.V. KRISHNAN: *Comparative Study of Spatial Domain Image Steganography Techniques*, International Journal Advanced Networking and Applications, **7**(2) (2015), 2650–2657.

[15] P. JAGOTA, S.E. GUPTA: *A Secure Image Steganography Technique based on Kekre's Algorithm*, International Journal of Advanced Research in Computer and Communication Engineering, **4**(9) (2015), 446–450.

[16] M.G. KACHERA, N. GAURAV JAIN: *An Improved Noise Resistant Image Steganography Technique Using Zero Cross Edge Detection Method*, International Research Journal of Engineering and Technology (IRJET). **4**(3) (2017). 1881–1886.

[17] A. SARKAR, S. KARFORMA: *Image Steganography using Password based Encryption Technique to secure e-Banking Data*, International Journal of Applied Engineering Research, **13**(22) (2018), 15477–15483.

[18] E. SARAVANA KUMAR, K. VENGATESAN, R.P. SINGH, C. RAJAN: *Biclustering of Gene Expression data using Biclustering Iterative Signature Algorithm and Biclustering Coherent Column*, International Journal of Biomedical Engineering and Technology, **26**(3-4) (2018), 341–352.

[19] E. SARAVANA KUMAR, K. VENGATESAN: *Trust based resource selection with optimization technique*, Cluster Comput **22** (2019), 207—213.

DEPARTMENT. OF COMPUTER SCIENCE AND ENGINEERING,
SRI SATYASAI UNIVERSITY OF TECHNOLOGY & MEDICAL SCIENCES,
SEHORE, BHOPAL-INDORE ROAD,
MADHYA PRADESH, INDIA.
Email address: sabyalnt@gmail.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
SRI SATYASAI UNIVERSITY OF TECHNOLOGY AND MEDICAL SCIENCES,
SEHORE, BHOPAL-INDORE ROAD,
MADHYA PRADESH, INDIA.