Computers, Materials & Continua
DOI: 10.32604/cmc.2022.028008
Article

Tech Science Press

Competitive Swarm Optimization with Encryption Based Steganography for Digital Image Security

Ala' A. Eshmawi[1], Suliman A. Alsuhibany[2], Sayed Abdel-Khalek[3] and Romany F. Mansour[4,*]

[1]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia
[2]Department of Computer Science, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia
[3]Department of Mathematics, College of Science, Taif University, Taif, 21944, Saudi Arabia
[4]Department of Mathematics, Faculty of Science, New Valley University, El-Kharga, 72511, Egypt
*Corresponding Author: Romany F. Mansour. Email: romanyf@sci.nvu.edu.eg
Received: 30 January 2022; Accepted: 02 March 2022

Abstract: Digital image security is a fundamental and tedious process on shared communication channels. Several methods have been employed for accomplishing security on digital image transmission, such as encryption, steganography, and watermarking. Image stenography and encryption are commonly used models to achieve improved security. Besides, optimal pixel selection process (OPSP) acts as a vital role in the encryption process. With this motivation, this study designs a new competitive swarm optimization with encryption based stenographic technique for digital image security, named CSOES-DIS technique. The proposed CSOES-DIS model aims to encrypt the secret image prior to the embedding process. In addition, the CSOES-DIS model applies a double chaotic digital image encryption (DCDIE) technique to encrypt the secret image, and then embedding method was implemented. Also, the OPSP can be carried out by the design of CSO algorithm and thereby increases the secrecy level. In order to portray the enhanced outcomes of the CSOES-DIS model, a comparative examination with recent methods is performed and the results reported the betterment of the CSOES-DIS model based on different measures.

Keywords: Image security; optimal pixel selection; encryption; metaheuristics; image steganography

1 Introduction

A Cryptography system is applied to encrypt the private information prior to embed inside the cover files. Image Steganography is exploited to hide information in an image [1]. Next, image selected for this act is called a cover-image, and image accomplished afterward steganography is denoted as stego-image. In Cryptography, 2 stages are comprised as Encryption and Decryption [2]. At first, encryption is determined as a procedure utilized for transforming the secret messages into an opaque format called cipher-text. Steganography is the task of hiding private messages by hiding their existence. In case of digital steganography, secured messages are covered with audio, image, video, etc.

In general, image is employed for cover media since the individual transmit digital images via internet communication and email schemes [3]. The authors didn't focus more on the problems such as when cover image dimension is unsuitable for creating image block to embed for performing information hiding and either this technique is prone to different kinds of stego attack [4]. Therefore, further methods needed to be applied namely modification to least amount of pixels or convert coefficient, usage of encrypted form of private message to be implanted [5]. Though, several works are needed for choosing appropriate trade-offs among the efficiency metrics like payload capacity, security, and imperceptibility. Now, secure information is transferred through text messages, images, videos, and audio files [6–8]. To forward this message in a hidden means, there is necessity for steganography. In the method, the embedded messages in the file are transported to the user at another end, whereby the message is unconcealed [9]. Though there are several software accessible online for data security, there is another software that can be used by hackers to decipher the secreted information [10]. Fig. 1 illustrates the process in image steganography.

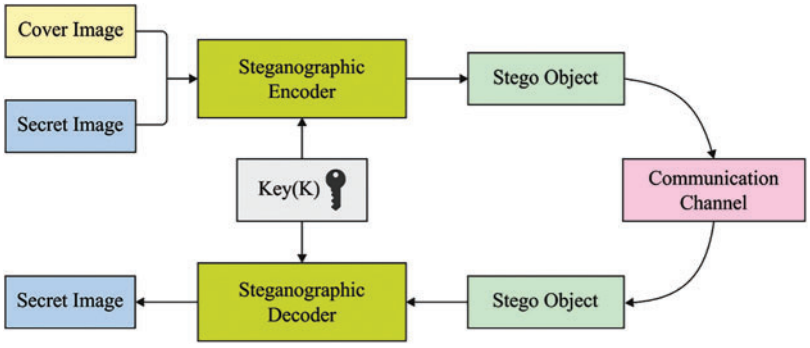

Figure 1: Process in image steganography

Parvees et al. [11] proposed an effective hybridization of fruit fly optimization (FFO) algorithm and Cat Swarm optimization algorithm (CSO) using ECC for image security, called CSO-FFO-ECC method. The presented approach implements the encryption and decryption method through ECC approach. Also, to minimize the computational time required for the arbitrary choice of the private and public keys, the suggested method employs a hybridization of CSO and FFO algorithm for optimum key choice. Hassaballah et al. [12] designed an approach named Harris hawks optimization-integer wavelet transform (HHO-IWT) for converting transmission and secured information from the IIoT environments related to digital image steganography. The approach embedded confidential information from the cover image with a metaheuristic optimization approach named HHO for effectively selecting image pixel that is utilized for hiding bits of secreted information with integer wavelet transform. The HHO-based pixel selection process utilizes a main functional assessment based on the subsequent two stages: exploration and exploitation phases.

Manjunath et al. [13] developed the audio steganography method for secured audio communication based on the metaheuristic model. In the embedding stage, the enhanced immediate selection is performed to embed the confidential message as to input audio. Moreover, the secreted messages that embedding was encoded by the enhanced 2D-Logistic Chaotic Map. The researchers in [14] presented an image Steganography with Secreted Share cryptography (SSC) was taken into account for upgrading the security level, now healthcare image is taken into account for stego image formation method. During the wake of inserting of secreted information with cover image Optimal Discrete Wavelet Transform (DWT) utilized for converting the region, now Daubechies (db2) coefficient is

employed, additionally, upgrade the PSNR Continual Harmony Search (CHS) applied for enhancing this coefficient. Finally, SS is performed for low band stego images with higher security procedures. Pandey [15] developed a bit mask oriented genetic approach (BMOGA) related secured medicinal data communication approach. The presented approach is employed for minimizing the replication of medicinal test data that is transported over organization. Healthcare information is taken into account as highly sensitive, thus secured medicinal data communication is essential. BOMGA exploits Boolean related mask-fill operator and performs reproduction operation in two distinct stages which assist in avoiding premature convergences.

This study designs a new competitive swarm optimization with encryption based stenographic technique for digital image security, named CSOES-DIS technique. The proposed CSOES-DIS model aims to encrypt the secret image prior to the embedding process. In addition, the CSOES-DIS model applies a double chaotic digital image encryption (DCDIE) technique to encrypt the secret image, and then embedded procedure was executed. Also, the OPSP can be carried out by the design of CSO algorithm and thereby increases the secrecy level. In order to portray the enhanced outcomes of the CSOES-DIS model, a comparative examination with recent methods is performed and results are investigated under several measures.

2 The Proposed Model

This study designs a new competitive swarm optimization with encryption based stenographic technique for digital image security, named CSOES-DIS technique. The proposed CSOES-DIS model aims to encrypt the secret image prior to the embedding process. In addition, the CSOES-DIS model applies a double chaotic digital image encryption (DCDIE) technique to encrypt the secret image, and then embedded method was executed. Also, the OPSP can be carried out by the design of CSO algorithm and thereby increases the secrecy level.

2.1 Encryption Using DCDIE Technique

At the initial stage, the secret image is encrypted by the use of DCDIE technique. To cryptographic structure of digital images, the plaintext space P is equivalent to group of pixels of a novel digital image which requires that encryption, and ciphertext spaces C equivalent to group of image pixels afterward the encrypted. The ciphertext spaces C obtianed with plaintext space P afterward encrypted is transferred from insecure channels. The key K is important to apply encrypt and decrypt transformed operations [16]. A similar key can be utilized to distinct encryption as well as decryption keys based on the selectively encrypted technique, or distinct keys are utilized. During the key space {K}, the control execution of encryption technique was recognized that is a space collected of fundamental data grasped by combined of plaintext as well as ciphertext spaces. These 2 chaotic series generators contained from the encrypted and decrypted procedures are the key elements of encrypted method. It can be responsible to realized of image encryption technique of the method. It can be executed by 2 chaotic maps, thus it is named as double chaotic digital image encrypt method, and other elements mostly contain the encryption as well as decryption element and broadcast component.

Encryption and decryption modules

An image encryption procedure of double chaotic digital image encrypts technique comprises of 2 procedures of confusion as well as scrambling procedure [16]. The confusion method is for XOR the pixel matrix of images with amount of pseudo-random order X and the scrambling approach is also handled by pseudo-random order information attained by logistic chaotic map. The confusion technique is as follows:

- Submitting the primary values a and b for pseudorandom sequence number (PSN) computation method, and fixed the computation parameter $\mu_1 = 3$ of L1 for calculating the PSN X.
- Compute each element of PSN from $(x_i \times 256)$ mod256, afterward converts the computed outcome as binary, so achieving a binary $M \times N$ long series number.
- Develop the pixel gray/color modules order of digital images that encryption and obtain the gray/color elements order vector G of digital images.
- In order to the primary element g_i from G, XOR was executed based on $X' \oplus g_i$. To succeeding element from G, it can be computed based on the subsequent equation:

$$I'(k) = X'^{(k)} \oplus \left\{\left[X'^{(k)} + g_k\right] mod\ N\right\} \oplus I'(k+1) \tag{1}$$

where k implies the k pixel from the image.

- Reversed the pixel sequence gained from the 4th step, change the novel $M \times N$ element to primary place, and alter the novel $M \times (N-1)$ element to secondary place. Next, based on Eq. (1), the secondary obfuscation procedure was implemented.

An image scrambling technique is as follows:

- Utilizing the PSN X of confusion approach as last set X of PSN.
- Utilizing the vector Y attained from preceding stage and the encrypting image I' afterward the confusion procedure, the pixel was scrambling to I'. Specifically, the gray value of i^{th} pixel as well as gray values of y_ith pixel from I' is replaced.
- The I was homogenization and empty vectors Y of $M \times N$ size is fixed, and X equivalent component is extended for integers domain space of $(0,\ M \times N)$ based on homogenized of X component, and the outcome was expressed to vector Y.
- The outcome of scrambling was over exposed for round of positive as well as revering sequences confusions based on the 4th and 5th steps from the confusion approach, so attaining the last encrypt image I''.

As per scrambling and confusion procedure, the double chaotic digital image encrypts method adapts the technique of primary confusing and afterward scrambled for encrypting images. The procedure of images decrypted was carried out by primary scrambling afterward confusion, and the function was inverse function of the above procedure. During the case of confusion inverse procedure, the succeeding techniques were utilized.

$$g_k = \{X'(k) \oplus I'(k) \oplus I'(k-1) - X'(k)\}\, mod\ N \tag{2}$$

2.2 CSO Based Pixel Selection Approach

In order to embed the secret image into the cover image, the optimal pixels are chosen by the design of CSO algorithm. CSO is the latest SI based technique, fundamentally simulated in PSO approach, but the model is extremely complex in typical PSO. During the CSO neither individual optimum nor global optimum are involved from the place upgrade process of particles. Assume that n amount of particles, $S(t)$ refers to that primary swarm. All the particles refer the potential solution. In order to all particles dimensional D is similar. The swarm $S(t)$ has n particles, from all iterations $n/2$ pairs are arbitrarily assigned, and then competition was developed amongst 2 from all the pairs of particles [17]. Thus the outcome of competition, the particle containing optimum fitness value, henceforth named as 'winner', is distributed directly to next iteration of swarms, $S(t+1)$, but the particle which loses the competition named as 'loser', is upgrading their velocity and position by learning in the winner. During all iterations, a particle contains after that competition. Specifically, to a swarm size of $n, n/2$

competition takes place and both namely velocity as well as position, of $n/2$ particles are only be upgraded. Assume that represent the velocity as well as position of winner and loser from m^{th} round of competitions from the iteration t with $V_{w,m}(t)$, $V_{l,m}(t)$, and $X_{w,m}(t)$, $X_{l,m}(t)$ correspondingly, where $m = 1, 2, 3, \ldots, n/2$. Fig. 2 demonstrates the search process of CSO technique.

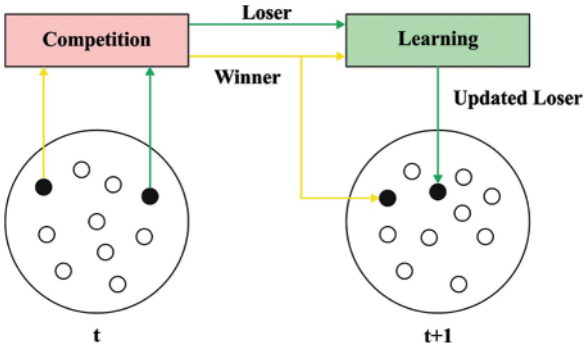

Figure 2: Search process of CSO algorithm

Based on the fundamental model of CSO, afterward m^{th} round of competitions the velocity as well as position of losers are upgraded utilizing subsequent learning methods:

$$V_{l,m}(t+1) = r_1(m,\ t) \times V_{l,m}(t) + r_2(m,\ t) \times \left(X_{w,m}(t) - X_{l,m}(t)\right) + \varphi \times r_3(m,\ t) \times \left(\bar{X} - X_{l,m}(t)\right) \quad (3)$$

$$X_{l,m}(t+1) = X_{l,m}(t) + V_{l,m}(t+1) \quad (4)$$

where, $r1(m,\ t)$, $r2(m,\ t)$ and $r3(m,\ t) \in [0, 1]$ and $\bar{X}(t)$ implies the mean position is determined from 2 approaches are global and local means represented as $\bar{X}_m^g(t) -$ and $X_l^g(t)$.$X_m^g(t)$ implies the global mean place of every particle, but $\bar{X}_l^g(t) -$ signifies the local mean of existing neighborhood of particles k.φ exist the parameter that controls the effect of $\bar{X}_m(t)$.

In order to optimum knowledge of CSO, it can project any connected comparative with PSO as follows [17]:

- A primary part $r1(m,\ t) \times V_{l,m}(t)$ is same as inertia term from typical PSO that balances the movement of swarms, the only variance is inertia weight w which is exchanged by an arbitrary vector $r_1(m, t)$ from CSO technique.
- The secondary part $r_2(m,\ t) \times \left(X_{w,m}(t) - X_{l,m}(t)\right)$ is same as the cognitive element from typical PSO technique, but, it can be conceptually extremely complex in typical PSO technique, the particle loses their competition learned in winner, before their individual optimum initiate to this point. This technique was further possible but inspiring performance of swarm, as it can be hard for remembering their individual optimum experience to this point.
- The tertiary part $r_3(m,\ t) \times \left(\bar{X}(t) - X_{l,m}(t)\right)$ is identical to the social element from typical PSO, but, particle lose competition learned in the mean position instead *gbest* from typical PSO, no memory has needed that is further possible biologically.

The FF was utilized to validate the quality of particles. The purpose of CSO is for finding the particle position which outcome optimum estimation of provided FF. All the particles are allocated with an arbitrary position as well as velocity from the initialized procedure of CSO technique. In CSO technique is most recent swarm optimized techniques dependent upon PSO. The CSO algorithm has derived a fitness function involving the maximization of PSNR. It can be represented as follows.

$$Fitness = max\{PSNR\} \tag{5}$$

2.3 Embedding and Extraction Process

For a provided covered image C, the encoding confidential communication ES was hidden as to cover image as follows. Primary, an IWT procedure was employed for transforming C in their spatial domain as to the frequency domains. The outcome of alteration was subdivision of images as to 4 subblocks (subbands) determined as high low (HL), high high (HH), low low (LL), and low high (LH), whereas ES is only embedding from the LH, HL, and HH subblocks as k bits from the k-LSBs of all pixels. Afterward hiding every confidential information from the particular subbands, the subband was fed as to OPAP for minimizing the variance amongst the altered coefficients and novel ones.

Afterward, the inverse transformation procedure of IWT was shown for combining the subbands composed again and creating the stegoimage. For removing the confidential communication, the stego-image was transformed to frequency domain utilizing IWT. Afterward, the k least significant bits are removed in all pixels of LH, HL, and HH subbands. The removed bits are encoder procedure ES. It can be decoder removal bits with encoder vector Ev for obtaining novel bits. Eventually, the bits are transformed for obtaining the confidential image S.

3 Experimental Validation

The experimental result analysis of the CSOES-DIS model is performed using benchmark images. The results are investigated interms of distinct measures. Some sample images are shown in Fig. 3.

Figure 3: (Continued)

Figure 3: Sample test images

Tab. 1 and Fig. 4 report the overall outcomes offered by the CSOES-DIS model for distinct cover and secret images. The experimental outcomes indicated that the CSOES-DIS model has accomplished effectual outcomes under all images. For instance, with cover image as 'Lena' and secret image as 'Lena', the CSOES-DIS model has attained MSE of 0.1400, RMSE of 0.3742, PSNR of 56.6695 dB, SSIM of 0.9984, and QI of 1.0000. Next, with cover image as 'Jet' and secret image as 'Jet', the CSOES-DIS model has attained MSE of 0.1800, RMSE of 0.4243, PSNR of 55.5781 dB, SSIM of 0.9983, and QI of 1.0000. In line with, with cover image as 'Boat' and secret image as 'Boat', the CSOES-DIS model has attained MSE of 0.2000, RMSE of 0.4472, PSNR of 55.1205 dB, SSIM of 0.9980, and QI of 1.0000.

Table 1: Overall steganography result analysis of CSOES-DIS model

Cover image	Secret image	MSE	RMSE	PSNR	SSIM	QI
Lena	Lena	0.1400	0.3742	56.6695	0.9984	1.0000
Baboon	Baboon	0.2300	0.4796	54.5135	0.9981	0.9990
Barbara	Barbara	0.2100	0.4583	54.9086	0.9982	0.9990
Jet	Jet	0.1800	0.4243	55.5781	0.9983	1.0000
Boat	Boat	0.2000	0.4472	55.1205	0.9980	1.0000

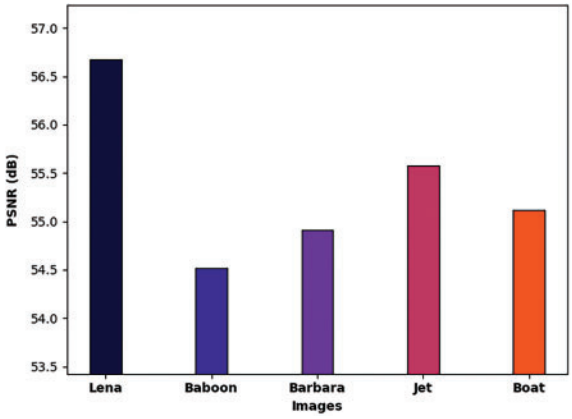

Figure 4: Steganography and encryption results of CSOES-DIS model

A brief computation time (CT) examination of the CSOES-DIS model is inspected under distinct cover images interms of embedding time (EBT), extraction time (EXT), and total time (TT) in Tab. 2 and Fig. 5. The results indicated that the CSOES-DIS model has gained minimal CT under all cover images. For instance, with cover image as 'Lena', the CSOES-DIS model has provided EBT, EXT, and TT of 0.4562, 0.3883, and 0.8445 min respectively. Moreover, with cover image as 'Jet', the CSOES-DIS model has achieved EBT, EXT, and TT of 0.4930, 0.3483, and 0.8413 min respectively. Furthermore, with cover image as 'Boat', the CSOES-DIS model has obtained EBT, EXT, and TT of 0.3998, 0.4437, and 0.8435 min respectively.

Table 2: CT analysis of CSOES-DIS model under various cover images

Computation time (min)			
Cover image	Embedding time	Extraction time	Total time
Lena	0.4562	0.3883	0.8445
Baboon	0.4192	0.4862	0.9053
Barbara	0.3555	0.4262	0.7817
Jet	0.4930	0.3483	0.8413
Boat	0.3998	0.4437	0.8435

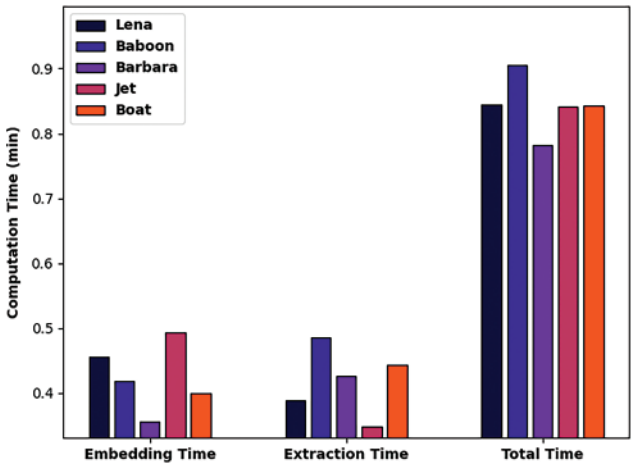

Figure 5: Comparative CT analysis of CSOES-DIS model under various cover images

A comparative PSNR study of the CSOES-DIS model is carried out with existing techniques under several cover images in Tab. 3 and Fig. 6. The results indicated that the CSOES-DIS model has resulted in higher PSNR values under all cover images. For instance, under 'Lena' image, the CSOES-DIS model has offered increased PSNR of 56.67 dB whereas the HPSM-WPT, AIS-HOG, IWT-PSO, and NIS-IITS models have obtained decreased PSNR values of 32.27, 36.32, 35.68, and 37.26 dB respectively. Meanwhile, under 'Boat' image, the CSOES-DIS model has accomplished higher PSNR of 55.12 dB whereas the HPSM-WPT, AIS-HOG, IWT-PSO, and NIS-IITS models have depicted lower PSNR values of 32.47, 35.95, 36.27, and 37.35 dB respectively.

Table 3: PSNR analysis of CSOES-DIS model under various cover images

PSNR (dB)					
Cover image	HPSM-WPT	AIS-HOG	IWT-PSO	NIS-IITS	CSOES-DIS
Lena	32.27	36.32	35.68	37.26	56.67
Baboon	32.89	35.91	36.34	37.25	54.51
Barbara	33.44	35.40	36.28	37.81	54.91
Jet	32.45	36.41	36.61	36.92	55.58
Boat	32.47	35.95	36.27	37.35	55.12

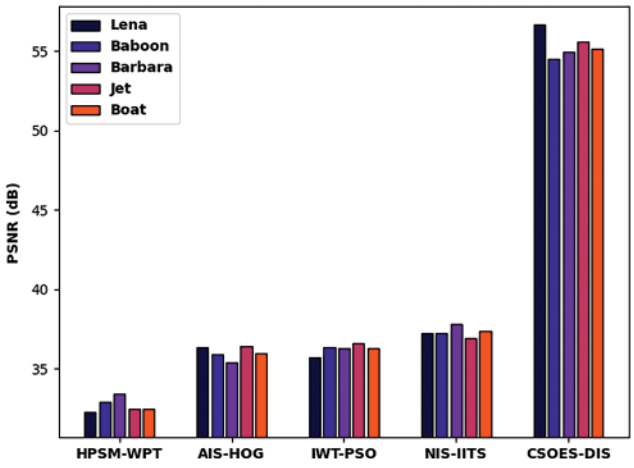

Figure 6: Comparative PSNR Analysis of CSOES-DIS model under various cover images

Finally, a comprehensive result analysis of the CSOES-DIS model under distinct kinds of attacks is provided in Tab. 4.

Table 4: Overall results of CSOES-DIS model under different kinds of attacks

Type of attacks	SC	NAE	EME	RMSE	PSNR	NCC	AD
Erosion	0.9965	0.5060	7.4169	9.8180	28.2903	0.9969	6.5751
Gaussian noise	0.9975	0.5270	7.5314	8.9320	29.1118	0.9981	6.4657
Dilation	0.9962	0.5360	7.7648	8.5020	29.5404	0.9979	6.5603
Salt & pepper noise	0.9965	0.5350	7.8287	8.5590	29.4823	0.9958	6.4449
Motion blur	0.9952	0.5080	7.8252	9.8700	28.2445	0.9976	6.7486

Fig. 7 offers a detailed SC examination of the CSOES-DIS model under various types of attacks. The figure portrayed that the CSOES-DIS model has attained increased values of SC under every attack. For instance, the CSOES-DIS model has achieved enhanced SC of 0.9956 under the existence of erosion attacks. Likewise, the CSOES-DIS model has attained improved SC of 0.9975 under the existence of Gaussian attack. Moreover, the CSOES-DIS model has obtained increased SC of 0.9962 under the existence of dilation attack. Furthermore, the CSOES-DIS model has demonstrated better SC of 0.9952 under the existence of motion blur attack.

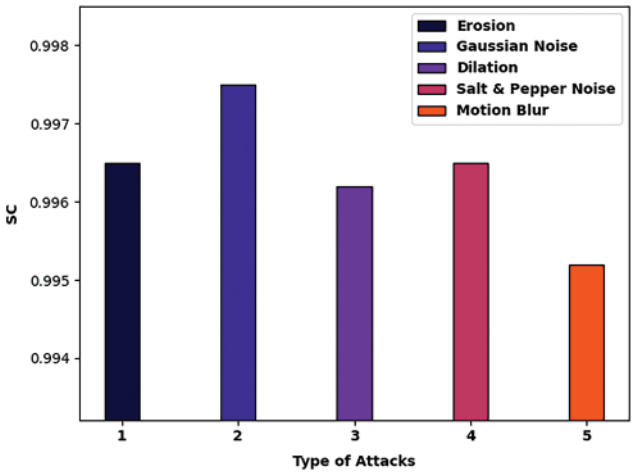

Figure 7: NC analysis of CSOES-DIS model under different kinds of attacks

Fig. 8 provides a brief NAE investigation of the CSOES-DIS model under numerous kinds of attacks. The figure depicted that the CSOES-DIS model has achieved increased values of NAE under every attack. For instance, the CSOES-DIS model has attained reduced NAE of 0.5060 under the existence of erosion attacks. Likewise, the CSOES-DIS model has accomplished effective NAE of 0.5270 under the existence of Gaussian attack. Besides, the CSOES-DIS model has gained NAE of 0.5360 under the existence of dilation attack. Also, the CSOES-DIS model has demonstrated NAE of 0.5080 under the existence of motion blur attack.

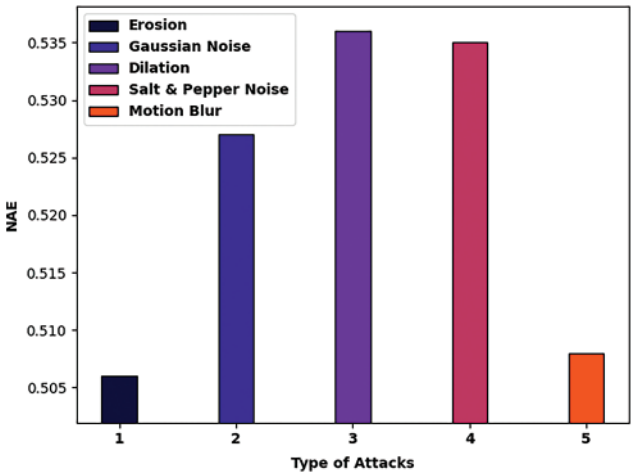

Figure 8: NC analysis of CSOES-DIS model under different kinds of attacks

Fig. 9 illustrates a comprehensive RMSE inspection of the CSOES-DIS model under various types of attacks. The figure portrayed that the CSOES-DIS model has reached increased values of RMSE under every attack. For instance, the CSOES-DIS model has achieved RMSE of 9.8180 under the existence of erosion attacks. Also, the CSOES-DIS model has attained RMSE of 8.9320 under the existence of Gaussian attack. Additionally, the CSOES-DIS model has obtained RMSE of 8.5020 under the existence of dilation attack. Also, the CSOES-DIS model has demonstrated better RMSE of 9.8700 under the existence of motion blur attack. After observing the detailed result analysis, it can be ensured that the CSOES-DIS model has accomplished better outcomes than the other methods.

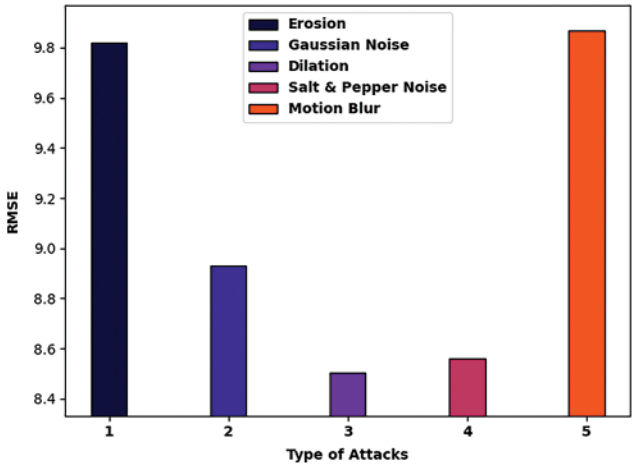

Figure 9: RMSE analysis of CSOES-DIS model under different kinds of attacks

4 Conclusion

In this study, a new CSOES-DIS technique has been developed for accomplishing maximum image security. It mainly intends to encrypt the secret image prior to the embedding process. Moreover, the DCDIE technique is applied for the encryption of secret images and then embedded into the cover image by the use of CSO based OPSP process. The OPSP can be carried out by the design of CSO algorithm and thereby increases the secrecy level. In order to portray the enhanced outcomes of the CSOES-DIS model, a comparative examination with recent methods is performed and results are investigated under several measures. The experimental results reported the betterment of the CSOES-DIS model based on different measures. In future, the CSOES-DIS technique can be placed in the real time healthcare environment for secured medical image transmission.

Funding Statement: Taif University Researchers Supporting Project Number (TURSP-2020/154), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim and H. M. Alzuabidi, "Combination of steganography and cryptography: A short survey," *IOP Conference Series: Materials Science and Engineering*, vol. 518, no. 5, pp. 052003, 2019.

[2] O. C. Abikoye, U. A. Ojo, J. B. Awotunde and R. O. Ogundokun, "A safe and secured iris template using steganography and cryptography," *Multimedia Tools and Applications*, vol. 79, no. 31–32, pp. 23483–23506, 2020.
[3] X. Duan, D. Guo, N. Liu, B. Li, M. Gou *et al.,* "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access*, vol. 8, pp. 25777–25788, 2020.
[4] R. Shanthakumari and S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," *Multimedia Tools and Applications*, vol. 79, no. 5–6, pp. 3975–3991, 2020.
[5] A. Gutub and F. Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2631–2644, 2020.
[6] F. Al-Shaarani and A. Gutub, "Securing matrix counting-based secret-sharing involving crypto steganography," *Journal of King Saud University-Computer and Information Sciences*, pp. S1319157821002603, 2021, Article in press, https://doi.org/10.1016/j.jksuci.2021.09.009.
[7] A. A. A. E. Latif, B. A. E. Atty and S. E. V. Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, pp. 92–102, 2019.
[8] M. R. Islam, T. R. Tanni, S. Parvin, M. J. Sultana and A. Siddiqa, "A modified LSB image steganography method using filtering algorithm and stream of password," *Information Security Journal: A Global Perspective*, vol. 30, no. 6, pp. 359–370, 2021.
[9] O. M. Osman, M. E. A. Kanona, M. K. Hassan, A. A. E. Elkhair and K. S. Mohamed, "Hybrid multistage framework for data manipulation by combining cryptography and steganography," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 327–335, 2022.
[10] R. Shanthakumari and S. Malliga, "Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment," *Sādhanā*, vol. 44, no. 5, pp. 119, 2019.
[11] M. M. Parvees and S. Kaliswaran, "An efficient hybrid optimization algorithm with elliptic-curve cryptography for image encryption," *European Journal of Molecular & Clinical Medicine*, vol. 7, no. 7, pp. 4753–4764, 2021.
[12] M. Hassaballah, M. A. Hameed, A. I. Awad and K. Muhammad, "A novel image steganography method for industrial internet of things security," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7743–7751, 2021.
[13] K. Manjunath, G. N. K. Ramaiah and M. N. GiriPrasad, "Backward movement oriented shark smell optimization-based audio steganography using encryption and compression strategies," *Digital Signal Processing*, vol. 122, pp. 103335, 2022.
[14] A. Sivasankari, and S. Krishnaveni, "Optimal wavelet coefficients based steganography for image security with secret sharing cryptography model," in *Cybersecurity and Secure Information Systems*, pp. 67–85, 2019, http://dx.doi.org/10.1007/978-3-030-16837-7_5.
[15] H. M. Pandey, "Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography," *Future Generation Computer Systems*, vol. 111, pp. 213–225, 2020.
[16] H. Pan, Y. Lei and C. Jian, "Research on digital image encryption algorithm based on double logistic chaotic map," *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 1, pp. 142, 2018.
[17] P. C. S. Rao, P. Lalwani, H. Banka and G. S. N. Rao, "Competitive swarm optimization based unequal clustering and routing algorithms (CSO-UCRA) for wireless sensor networks," *Multimedia Tools and Applications*, vol. 80, no. 17, pp. 26093–26119, 2021.