



Modeling of Multiple Share Creation with Optimal Signcryption Technique for Digital Image Security

Abdul Rahaman Wahab Sait¹, Irina Pustokhina², M. Ilayaraja³

¹ King Faisal University, Kingdom of Saudi Arabia

² Plekhanov Russian University of Economics, Moscow, Russia

³ Department of Computer Science and Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, India

Emails: asait@kfu.edu.sa; ivpustokhina@yandex.ru, ilayaraja.m@klu.ac.in

Abstract

Digital image security plays an essential role in the shared communication model. The encryption and decryption process is commonly applied to securely transmit the images in various real-time applications. In addition, the generation of encryption/decryption keys is also essential to achieve enhanced image security. This study presents a multiple share creation scheme with an optimal signcryption (MSS-OSC) technique for digital image security. The MSS-OSC technique primarily generates a set of various shares for every digital image that needs to be transmitted. In addition, the encryption of generated shares takes place via the optimal signcryption (OSC) technique. Moreover, genetic programming (GP) is employed to optimally choose the keys involved in the encryption and decryption process. The detailed experimental validation of the MSS-OSC technique is investigated using a set of benchmark test images. The results analysis demonstrated that the MSS-OSC technique had a superior performance by accomplishing maximum digital image security.

Keywords: Digital image security; Signcryption; Share creation; Encryption; Optimal key generation; Genetic programming.

1. Introduction

Information security is determined as the area of investigation aiming to defend data from malicious hackers since it permits legal users to control information. Various privacy factors consist of several risks, and cryptography isn't adequate alone [1]. The concept of data security resulted in the development of Cryptography and also the science of keeping the data to be secure. It should include the encryption procedure and decryption methods of an image. Several well-known cryptographic algorithms exist. A significant portion of cryptography is the "key" utilized to encrypt and decrypt the data. Although few institutions consider the method a max-out secret [2]. The digital image is useful datatype with a wider variety of users. Several users are stimulated to execute content security methods on their image to save it from direction and preview. Hence, several application exists according to images. The vital tasks of an image in business processes are attracted to resources. Therefore, it is essential to preserve private images from unauthorized attacks [3].

Cryptography is the science of concealing data that is exposed only by the genuine user. It provides privacy for transferred information on an unsecured network and avoids data tampering and eavesdropping. Another landscape, cryptanalyses, is considered by decrypting and attacking with this cipher information [4]. Abundant cryptography systems are designed and utilized to secure information;

few use distributed key cryptography, and others use Public Key Cryptography (PKC). Distributed key cryptography is a scheme that employs a single key with receiver and sender to decrypt and encrypt communications. Public cryptography uses two individual keys termed public keys and private-key.

Image privacy is becoming increasingly significant as growing amounts of categorized images are transferred on the public Internet or consumed in a 3rd parties [5]. With this respect, different image cryptosystems are suggested since the encryption is viewed as an effective and direct method for guarding personal information [6]. Decryption and Encryption of information have resulted in the optimal method for getting respectability and secrecy of data. Eventually, there is a key test as vulnerabilities and dangers extend with progress development [7]. Nowadays, distinct methods are raised to provide security, make a high rate, and use computation resources. Image encryption methods encourage to alter of single images to other images (encoded) which is not direct; alongside this line, to preserve this image confidentiality among the users, in other words, it is important that nobody has to turn out to be more familiar using the substances without keys for the decryption method.

This study presents a multiple share creation scheme with an optimal signcryption (MSS-OSC) technique for digital image security. The MSS-OSC technique primarily generates a set of various shares for every digital image that needs to be transmitted. In addition, the encryption of generated shares takes place via the optimal signcryption (OSC) technique. Moreover, genetic programming (GP) is employed to optimally choose the keys involved in the encryption and decryption process. The detailed experimental validation of the MSS-OSC technique is investigated using a set of benchmark test images. The results analysis demonstrated that the MSS-OSC technique had a superior performance by accomplishing maximum digital image security.

2. Related works

In Avudaiappan et al. [8], a dual encryption process has been employed for encrypting the medicinal image. Primarily, the Blowfish Encryption has been regarded, and afterward, signcryption technique was employed for confirming the encryption technique. Then, Opposition-based Flower Pollination (OFF) has been employed to upgrade the private and public keys. Kankonkar and Naik [9] offer security to the image by utilizing image encryption and image stitching approaches. It can be used as chaotic approaches from the encrypted create further complexity for the attacker to decrypt the images. All the transmitted images were initially separated, and all the parts were then encrypted and sent to the receiver. The person with a single or two parts of an image could not utilize that image. An image stitching technique used on the receiver end generated it simple for him for generating the original images.

Ilaga et al. [10] presented the ECB Mode cryptographic technique and LSB steganographic technique on digital images. The measurement technique has PSNR and MSE for determining the quality of stego images. Saranya et al. [11] established an effectual image encryption technique with enhanced image security by utilizing chaotic functions, deoxyribonucleic acid (DNA) sequence, and GA. The chaotic sequences of the desired length have been created utilizing the logistic map function whose primary value has been computed using the confidential keys. The amount of DNA mask has been created, and this mask and the chaotic sequence have been utilized for encrypting the digital image. Eventually, the GA has been utilized for getting an optimum mask to encrypt.

Rajput and Nishchal [12] present a new security method dependent upon the double random phase fractional domain encoding (DRPE) and modified Gerchberg-Saxton (G-S) stage retrieval technique to secure two images concurrently. By anyone image that encryption has been changed to phase-only images utilizing a modified G-S technique, and this function has been used as a key to encrypt another image. In Saranya et al. [13], an image encryption technique dependent upon chaotic theory and DNA sequences is presented at this point. Primarily, two chaotic sequences have been created in the logistic map function, one to image permutation and another to image diffusions. The two internal confidential keys resultant in the 120bit user-defined confidential key serve as the chaotic sequence's primary criteria. Combined image and mask to diffusion were encoded into DNA sequence utilizing the feasible 8 DNA complementary rules.

In Ramya et al. [14], the image occur secured has been watermarked utilizing the watermark images and afterward encryption with S-DES (Simple-Data Encryption Standard) technique. This encrypted image has been decrypted by executing S-DES decryption initial and then eliminating the watermark. Also, an image security technique confirms the confidentiality of the images. In Brar and Brar [15], the hybrid image security structure was presented for overcoming this issue stated previously that has been executed as joining several approaches composed for attaining the image security aim. The approaches contained in the joined have been image compression, cryptography, and steganography. The DWT compression was utilized as it can be a more robust compression technique.

3. Design of MSS-OSC Technique

The proposed MSS-OSC technique involves a three-stage process: share creation, share encryption, and optimal key generation. Through these three processes, the MSS-OSC technique can attain improved security.

3.1 Steps involved in Share Creation Model

The pixel values of the original image are obtained, and the RGB value is demonstrated in a matrix [16]. The size of the matrix corresponds to an input image size ($X*Y$). So, the original pixel value of implemented image was calculated in Eq. (1):

$$Pixel = \sum R + G + B \quad (1)$$

Where *pixel* represents the sum of R, G , and B , the pixels that occur in the executed image are demonstrated from the procedure of n changed manners named as shares. All the shares contain the set of subpixels of an input image. The R, G , and B shares depend on the advanced pixel value from the RGB images. The shares of the executed image are independently determined as R_s, G_s , and B_s in Eqs. (2)-(4),

$$R_s = \int_1^k \lim_{k \rightarrow 1ton} R_{ab} \quad (2)$$

$$G_s = \int_1^k \lim_{k \rightarrow 1ton} G_{ab} \quad (3)$$

$$B_s = \int_1^k \lim_{k \rightarrow 1ton} B_{ab} \quad (4)$$

where a and b imply the places of the matrix, R_s, G_s , and B_s stand for the shares of RGB, R_{ab}, G_{ab} , and B_{ab} , which are the element of pixel value from the image. The RGB pixel values are formed in the input image and retained as the distinct matrix. Then, the shares are generated depending on the partitions of the image to diverse regions. The MSC approach alters the image to many shares that don't contain meaningful details unless all shares are related.

Previous to generating shares, the fundamental matrices are adjusted the user could set that. Also, an arbitrary key has been provided based on the input image's block size, which is 4×4 or 8×8 . The entire amount of shares is kept as 2^s if the $S \geq 2$. The fundamental matrix was attained once the RGB value of the pixel was separated by S . Afterward, the shares were created utilizing the XOR function of basic matrixes on several combinations.

For the sample, consider that the block of size $2*2$, the RGB values are determined as:

$$R = \begin{bmatrix} 126 & 230 & 46 \\ 32 & 60 & 134 \end{bmatrix},$$

$$G = \begin{bmatrix} 39 & 42 & 64 \\ 121 & 31 & 184 \end{bmatrix},$$

$$B = \begin{bmatrix} 94 & 106 & 109 \\ 76 & 83 & 241 \end{bmatrix}$$

Besides, the key matrix K_M is arbitrarily created as follows.

$$K_M = \begin{bmatrix} 61 & 92 & 87 \\ 34 & 81 & 140 \end{bmatrix}$$

The simple matrix count is two, and the share count is four. The simple matrix has been resulted by separating the RGB values of pixel by 2. Next, the basic matrices are resultant utilizing existing models, which are demonstrated as B_{M1} and B_{M2} correspondingly.

$$B_{M1} = \begin{bmatrix} 63 & 115 & 23 \\ 16 & 30 & 67 \end{bmatrix},$$

$$B_{M2} = \begin{bmatrix} 63 & 115 & 23 \\ 16 & 30 & 67 \end{bmatrix}$$

Previously share creation, the following functions are taking place on the XR_1 and XR_2 matrices.

$$\begin{aligned} XR_1 &= 128 - B_{M1} \\ XR_2 &= B_{M2} \end{aligned} \quad (5)$$

$$XR_1 = \begin{bmatrix} 65 & 13 & 105 \\ 112 & 98 & 61 \end{bmatrix},$$

$$XR_2 = \begin{bmatrix} 63 & 115 & 23 \\ 16 & 30 & 67 \end{bmatrix}$$

The red band shares have been formed by implementing the XOR function amongst the primary and key matrixes.

$$Rs1 = XR_1 \oplus K_M$$

$$Rs2 = XR_2 \oplus XR_1 \quad (6)$$

$$Rs3 = XR_2 \oplus Rs1$$

$$Rs4 = Rs1 \oplus R$$

$$Rs1 = \begin{bmatrix} 124 & 81 & 62 \\ 82 & 51 & 177 \end{bmatrix},$$

$$Rs2 = \begin{bmatrix} 126 & 126 & 126 \\ 96 & 124 & 126 \end{bmatrix},$$

$$Rs3 = \begin{bmatrix} 67 & 34 & 41 \\ 66 & 45 & 242 \end{bmatrix},$$

$$Rs4 = \begin{bmatrix} 2 & 183 & 16 \\ 114 & 15 & 55 \end{bmatrix}$$

The beyond procedure obtains repeating to other green as well as blue bands for creating several shares.

At the receiver end, every multiple shares are both together creating an input image,

$$R = Rs1 \oplus Rs2 \oplus Rs3 \oplus Rs4 \oplus Rs4 \oplus K_M$$

$$G = Gs1 \oplus Gs2 \oplus Gs3 \oplus Gs4 \oplus Gs4 \oplus K_M \quad (7)$$

$$B = Bs1 \oplus Bs2 \oplus Bs3 \oplus Bs4 \oplus Bs4 \oplus K_M$$

Afterward, the reconstructed red band share is provided as:

$$R = \begin{bmatrix} 126 & 230 & 46 \\ 32 & 60 & 134 \end{bmatrix}$$

Once the shares are created and the encryption procedure is completed on the color band of the shares by the OSC technique. All the color bands of images are separated as a group of blocks previous to encrypted, and the blocks are separated as to the size of 4×4 .

3.2 Steps involved in OSC Technique

Afterward, the OSC methodology was implemented for encrypting the image, and the optimal production of keys was applied by the GP technique. Signcryption has been determined as a public-key cryptosystem that gives appropriate protection to secret images in the production of electronic signatures and encryption. The variable implemented from Signcryption method has been sender 'S', standard parameters 'cp', confidential key of sender 'xs', the public key of receivers 'yr' and sender as well as receiver public keys 'ys', 'yr' as 'binfo' are determined as inputs to Signcryption manner. Fig. 1 illustrates the Signcryption Process. The variable 'binfo' was essential for protecting the Signcryption, which comprised strings utilized to find the transmitter and receiver public keys hash value [17].

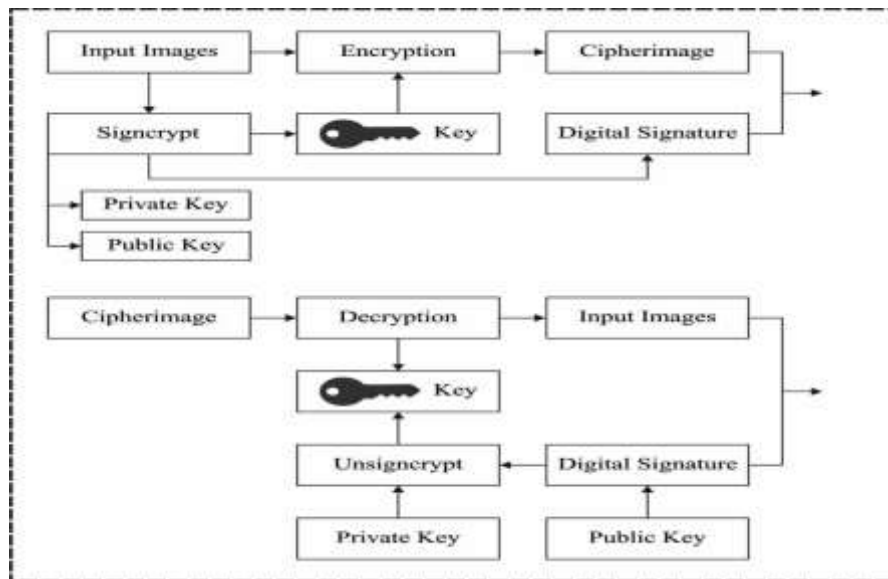


Figure 1: Signcryption Process

The optimal keys are chosen by the GP approach. GP is a kind of evolutionary algorithm (EA) that generalizes the genetic model. GP is an algorithm to test and select the optimal selection amongst a collection of outcomes. GP generates a resolution according to the fundamental mechanism and biological evolution (selection, mutation, and crossover). The usage of GP is the cause for its flexibility; it could design a system wherein the framework of the desirable methods and the main feature is unknown. In this work, GP permitted the scheme to seek models from a range of potential models and optimize the pipeline denoted in a tree structure for the classifier problems. First, GP generates a static pipeline depending on the primitive defined previously, like feature selection decomposition. In other words, the series of workers evolve to produce an ML pipeline, which is calculated to maximize the classification performance. Afterward, calculation of the present pipeline ML, a novel generation is made according to the maximum prior pipeline. All the pipelines are taken into account by a single GP [18]. The GP is made using the three major operators:

Mutation operator: altering hyperparameter or removing or adding primitive preprocessing steps like Standard Scaler or the tree count in RF.

The crossover operator assumes that 5% of individuals would cross over one another by a 1-point crossover chosen at random.

Selection operator: its primary goal is to choose the topmost twenty individuals and create copies from them. To interchange data among the individual populations, the mutation/crossover operators were employed.

4. Performance Evaluation

The results analysis of the MSS-OSC approach takes place using benchmark test images, and the results are inspected under different measures. Fig. 2 depicts a few sample images.



Figure 2: Sample images

Table 1 provides the performance validation of the MSS-OSC technique in terms of MSE and PSNR.

Table 1: Result Analysis of Proposed MSS-OSC Model concerning MSE and PSNR

Test Images	MSE			PSNR		
	MSS-OSC	WOA	GWO	MSS-OSC	WOA	GWO
Image 1	0.105	0.251	0.541	57.92	54.13	50.80
Image 2	0.103	0.37	0.495	58.00	52.45	51.18
Image 3	0.135	0.282	0.595	56.83	53.63	50.39
Image 4	0.122	0.202	0.429	57.27	55.08	51.81
Image 5	0.134	0.345	0.525	56.86	52.75	50.93

Fig. 3 portrays the MSE analysis of the MSS-OSC approach with existing algorithms. The figure has shown that the MSS-OSC approach has gained a lower MSE value and exhibited improved outcomes. For instance, with image 1, the MSS-OSC technique has a minimal MSE of 0.105, whereas the WOA and GWO techniques have obtained a maximum MSE of 0.251 and 0.541. Similarly, with image 2, the MSS-OSC technique has attained a lower MSE of 0.103, whereas the WOA and GWO techniques have gained a higher MSE of 0.37 and 0.495. Also, with image 3, the MSS-OSC technique has reached a lesser MSE of 0.135, whereas the WOA and GWO techniques have attained a maximum MSE of 0.282 and 0.595. At last, with image 5, the MSS-OSC technique has reached a minimal MSE of 0.134, whereas the WOA and GWO systems have gained a maximal MSE of 0.345 and 0.525.

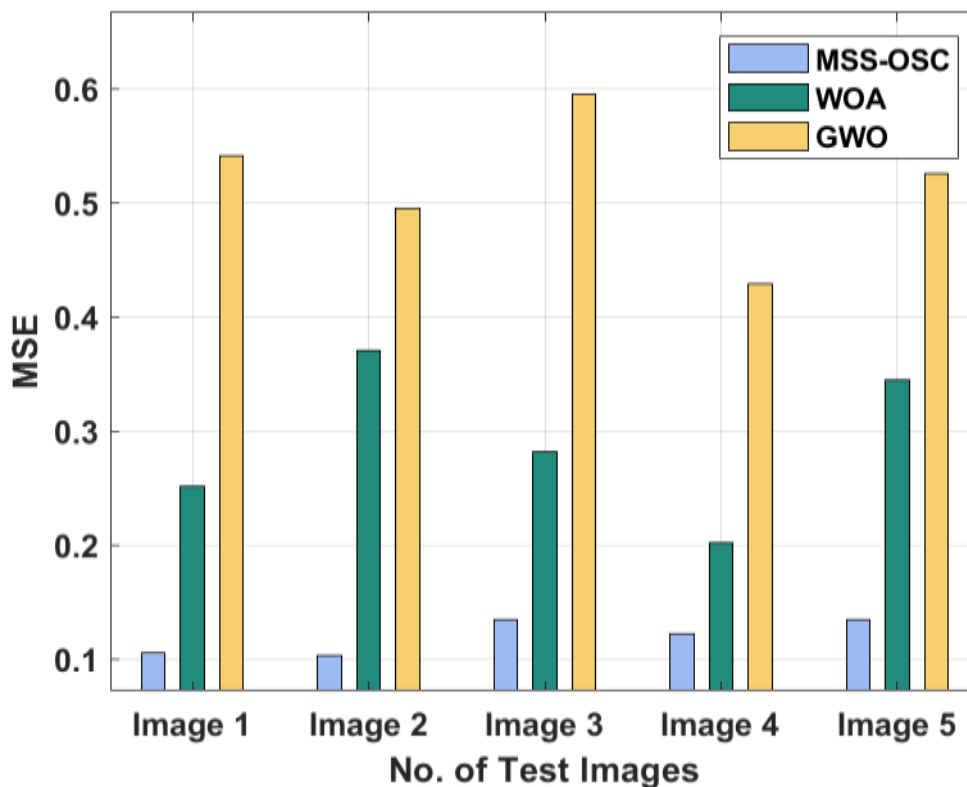


Figure 3: MSE analysis of MSS-OSC model with varying images

The PSNR analysis of the MSS-OSC approach with other techniques is performed in Fig. 4. The results showcased that the MSS-OSC approach has resulted in increased PSNR values compared to other appraises. For instance, with image 1, the MSS-OSC technique has increased PSNR by 57.92dB, whereas the WOA and GWO techniques have exhibited a reduced PSNR of 54.13dB and 50.80dB. Likewise, with image 2, the MSS-OSC technique has an enhanced PSNR of 58dB, whereas the WOA and GWO techniques have showcased a decreased PSNR of 52.45dB and 51.18dB. Simultaneously, with image 3, the MSS-OSC system has an increased PSNR of 56.83dB, whereas the WOA and GWO techniques have exhibited a reduced PSNR of 53.63dB and 50.39dB. Eventually, with image 5, the MSS-OSC manner has improved PSNR of 56.86dB, whereas the WOA and GWO algorithms have portrayed a minimum PSNR of 52.75dB and 50.93dB.

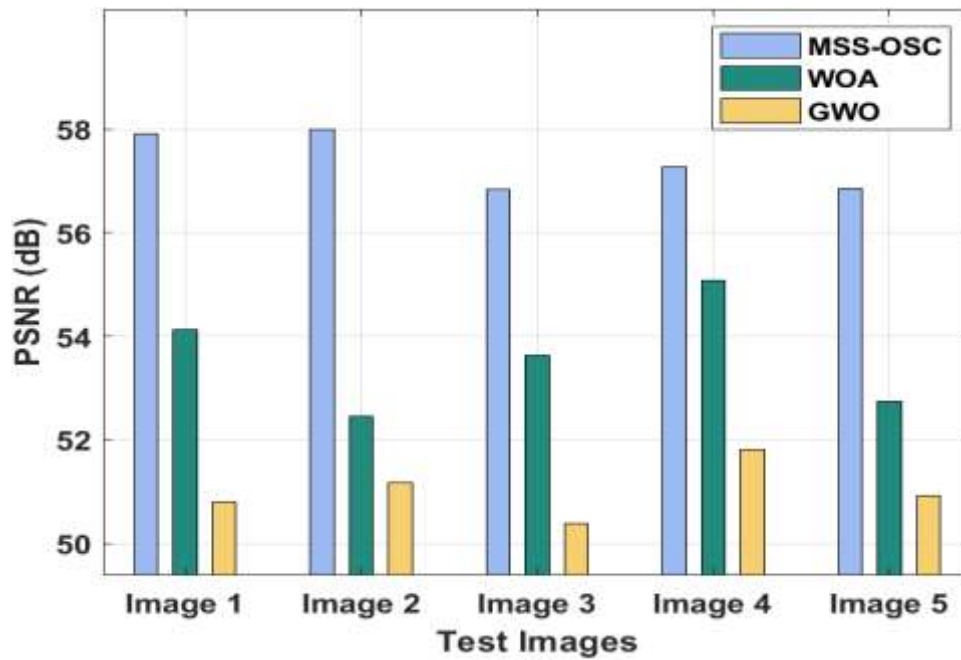


Figure 4: PSNR analysis of MSS-OSC model with varying images

Table 2 offers the performance validation of the MSS-OSC algorithm in terms of NCC and SSIM.

The NCC analysis of the MSS-OSC manner with other algorithms is implemented in Fig. 5. The results demonstrated that the MSS-OSC approach has resulted in increased NCC values compared to other appraisals. For instance, with image 1, the MSS-OSC technique has increased NCC by 0.998, whereas the WOA and GWO techniques have exhibited a reduced NCC of 0.991 and 0.972. In line with image 2, the MSS-OSC scheme has accomplished a higher NCC of 0.997, whereas the WOA and GWO systems have exhibited a reduced NCC of 0.986 and 0.963. Simultaneously, with image 3, the MSS-OSC technique has increased NCC by 0.996, whereas the WOA and GWO methods have reduced NCC by 0.976 and 0.951. Finally, with image 5, the MSS-OSC technique has increased NCC to 0.997, whereas the WOA and GWO manners have demonstrated a minimum NCC of 0.989 and 0.982.

Table 2: Result Analysis of Proposed MSS-OSC Model concerning NCC and SSIM

Test Images	NCC			SSIM		
	MSS-OSC	WOA	GWO	MSS-OSC	WOA	GWO
Image 1	0.998	0.991	0.972	0.970	0.958	0.952
Image 2	0.997	0.986	0.963	0.980	0.971	0.957
Image 3	0.996	0.976	0.951	0.980	0.961	0.956
Image 4	0.995	0.990	0.976	0.980	0.958	0.938
Image 5	0.997	0.989	0.982	0.960	0.941	0.932

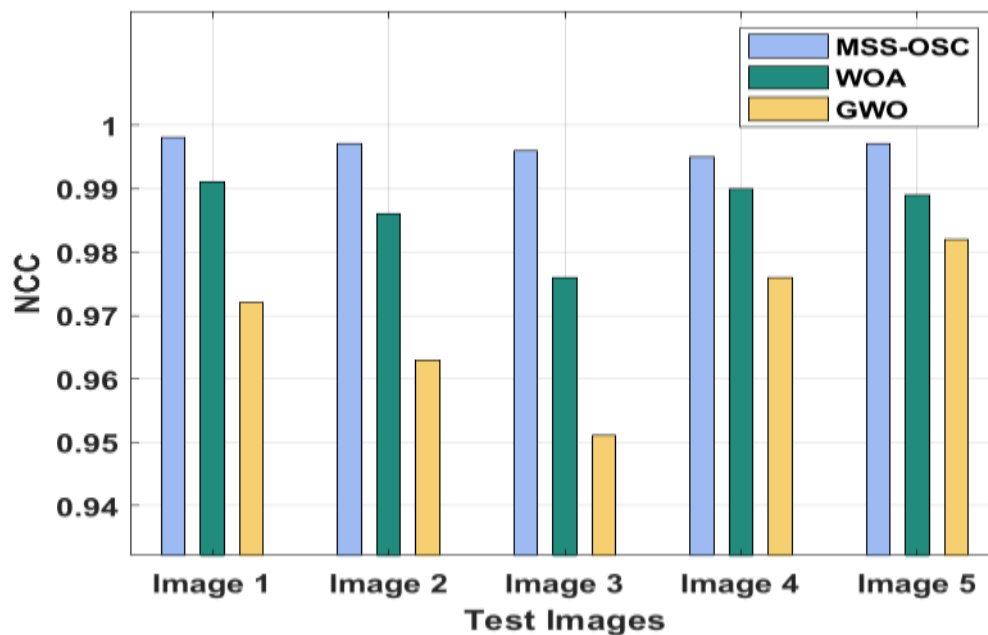


Figure 5: NCC analysis of MSS-OSC model with varying images

The SSIM analysis of the MSS-OSC approach with other manners is carried out in Fig. 6. The results illustrated showcased that the MSS-OSC approach has resulted in enhanced SSIM values compared to other appraisals. For instance, with image 1, the MSS-OSC technique has increased SSIM by 0.970, whereas the WOA and GWO manners have exhibited a minimum SSIM of 0.958 and 0.952. Similarly, with image 2, the MSS-OSC algorithm has increased SSIM by 0.980, whereas the WOA and GWO techniques have exhibited a reduced SSIM of 0.971 and 0.957. Concurrently, with image 3, the MSS-OSC approach has accomplished an enhanced SSIM of 0.980, whereas the WOA and GWO methods have exhibited a lower SSIM of 0.961 and 0.956. At last, with image 5, the MSS-OSC technique has accomplished an increased SSIM of 0.960, whereas the WOA and GWO approaches have outperformed a minimum SSIM of 0.941 and 0.932.

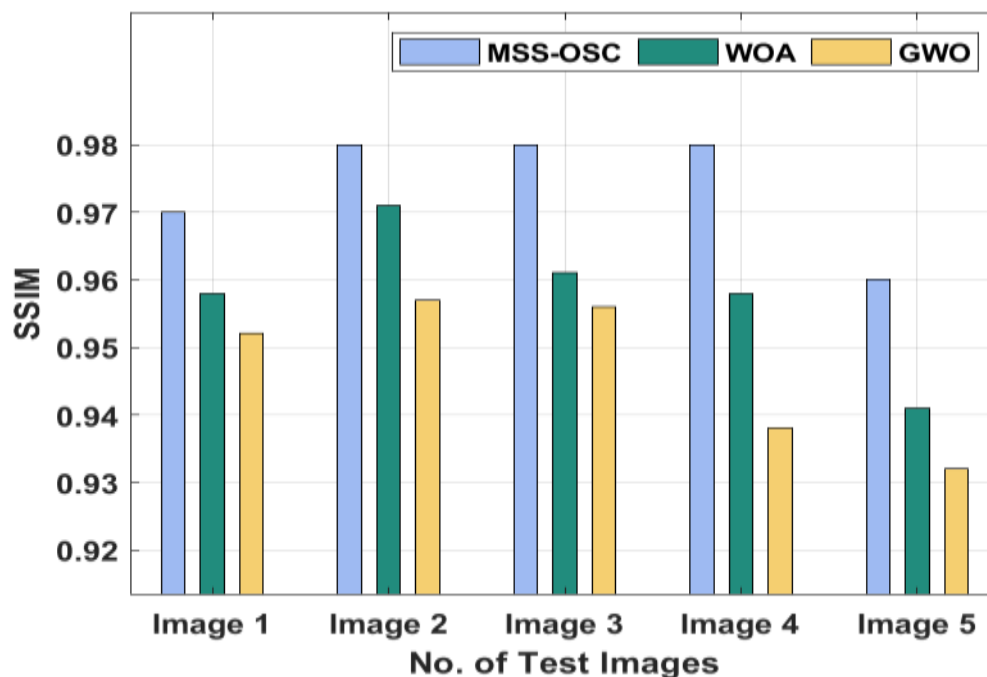


Figure 6: SSIM analysis of MSS-OSC model with varying images

5. Conclusion

This paper has presented a new MSS-OSC technique to accomplish maximum digital image security. The MSS-OSC technique primarily generates a set of multiple shares for every digital image that needs to be transmitted. In addition, the encryption of generated shares takes place via the OSC technique. Furthermore, the GP approach performs the optimal key generation process for the encryption/decryption process. The detailed experimental validation of the MSS-OSC technique is investigated using a set of benchmark test images. The results analysis demonstrated that the MSS-OSC technique had a superior performance by accomplishing maximum digital image security. In the future, the MSS-OSC technique can be extended to the design of image steganography techniques.

References

- [1] Razzaq, M.A., Sheikh, R.A., Baig, A. and Ahmad, A., 2017. Digital image security: Fusion of encryption, steganography, and watermarking. *International Journal of Advanced Computer Science and Applications*, 8(5), pp.224-228.
- [2] Shankar, K. and Lakshmanprabu, S.K., 2018. Optimal key-based homomorphic encryption for color image security aid of ant lion optimization algorithm. *International Journal of Engineering & Technology*, 7(9), pp.22-27.
- [3] Liu, Y., Tang, S., Liu, R., Zhang, L., and Ma, Z., 2018. Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, 97, pp.95-105.
- [4] Dorothy, A.B., Kumar, S.B.R. and Sharmila, J.J., 2017, February. IoT based home security through digital image processing algorithms. In *2017 World Congress on Computing and Communication Technologies (WCCCT)* (pp. 20-23). IEEE.
- [5] Loan, N.A., Hurrah, N.N., Parah, S.A., Lee, J.W., Sheikh, J.A. and Bhat, G.M., 2018. Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access*, 6, pp.19876-19897.
- [6] Ardy, R.D., Indriani, O.R., Sari, C.A. and Rachmawanto, E.H., 2017, November. Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5). In *2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS)* (pp. 87-92). IEEE.
- [7] Mehran, N. and Khayyambashi, M.R., 2017. Performance evaluation of authentication-encryption and confidentiality block cipher modes of operation on digital image. *International Journal of Computer Network and Information Security*, 11(9), p.30.
- [8] Avudaiappan, T., Balasubramanian, R., Pandiyan, S.S., Saravanan, M., Lakshmanprabu, S.K. and Shankar, K., 2018. Medical image security using dual encryption with oppositional based optimization algorithm. *Journal of medical systems*, 42(11), pp.1-11.
- [9] Kankonkar, J.T. and Naik, N., 2017, July. Image security using image encryption and image stitching. In *2017 International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 151-154). IEEE.
- [10] Ilaga, K.R., Sari, C.A. and Rachmawanto, E.H., 2018. A high result for image security using cryptostegano based on ECB mode and LSB encryption. *Journal of Applied Intelligent System*, 3(1), pp.28-38.
- [11] Saranya, M.R., Mohan, A.K. and Anusudha, K., 2015, February. Algorithm for enhanced image security using DNA and genetic algorithm. In *2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)* (pp. 1-5). IEEE.
- [12] Rajput, S.K. and Nishchal, N.K., 2017. Optical double image security using random phase fractional Fourier domain encoding and phase-retrieval algorithm. *Optics Communications*, 388, pp.38-46.
- [13] Saranya, M.R., Mohan, A.K. and Anusudha, K., 2015, January. A hybrid algorithm for enhanced image security using chaos and DNA theory. In *2015 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-4). IEEE.
- [14] Ramya, M.S., Soman, P.S. and Deepthi, L.R., 2017, September. A novel approach for image security using reversible watermarking. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 338-343). IEEE.
- [15] Brar, S.S. and Brar, A., 2016. Double Layer Image Security System using Encryption and Steganography. *International Journal of Computer Network & Information Security*, 8(3).

- [16] Forrester, P.L., Shimizu, U.K., Soriano- Meier, H., Garza- Reyes, J.A. and Basso, L.F.C., 2010. Lean production, market share and value creation in the agricultural machinery sector in Brazil. *Journal of Manufacturing Technology Management*.
- [17] Li, F.G., Masaaki, S. and Tsuyoshi, T., 2008. Analysis and improvement of authenticatable ring signcryption scheme. *Journal of Shanghai Jiaotong University (Science)*, 13(6), pp.679-683.
- [18] Brameier, M. and Banzhaf, W., 2001. A comparison of linear genetic programming and neural networks in medical data mining. *IEEE Transactions on Evolutionary Computation*, 5(1), pp.17-26.