International Journal of Engineering & Technology, 7 (1.9) (2018) 22-27

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm

Shankar K [1] *, Lakshmanaprabu S. K [2]

[1] Assistant Professor, School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, India
[2] Research Scholar, Department of Electronics and Instrumentation Engineering, BS Abdur Rahman
Crescent Institute of science and Technology, Chennai, India
**Corresponding author E-mail: shankar.k@klu.ac.in*

Abstract

The security of digital images is a basic and difficult task on the shared communication channel. Different strategies are utilized to secure the digital image, for example, encryption, steganography and watermarking. These are the techniques for the security of digital image to accomplish security objectives, i.e. secrecy, trustworthiness, and accessibility. In the proposed study, Homomorphic Encryption (HE) with optimal key selection for image security is utilized. Here the histogram equalization is introduced for altering image intensities to improve contrast. The histogram of an image generally speaks to the comparative frequency of occurrence of the different gray levels in the image. To increase the security level inspired Ant Lion Optimization (ALO) is considered, where the fitness function as max entropy the best-encrypted image is characterized as the image with most astounding entropy among adjacent pixels. Analyzing the outcomes from the performed experimental outcomes can accomplish abnormal state and great strength of proposed model compared with other encryption strategies.

Keywords: *Ant Lion Optimization; Decryption; Encryption; Entropy; Homomorphic Encryption; Image Security*.

1. Introduction

In the recent period of communication field, digital image applications have been significantly rising more common than the earlier [1]. Cryptographic methods are crucial for ongoing safe image communication [2]. Most recently, image security is ending up progressively important as an ever-increasing number of classified images are transmitted over the public Internet or put away in a third party [3]. In this regard, different image cryptosystems recommended because encryption is perceived as a successful and direct procedure to guard private data [4]. Encryption and decryption of data have ended up being the ideal approach to get secrecy and respectability of information. By and by, there is a major test since dangers and vulnerabilities are expanding with the improvement of advances [5]. These days, distinctive algorithms elevated to give security yet in the meantime, create a higher cost and utilization of computational assets. image encryption strategies encourages us to change unique image to another image (encoded) [6] that isn't straightforward; along these lines, to keep the picture secret between clients, in other word, it is fundamental that no one could become more acquainted with the substance without a key for decryption [7].

Homomorphic cryptosystems are extraordinary sorts of cryptosystems with a limit of accomplishing development and increase process on mixed data choice of revealing any information concerning interesting data [8].Homomorphic Encryption used as a section of the request to shield the shared pictures from the capture attempt in the midst of transmission with limit and in addition combine the encoded pictures to outline another picture to reduce the information exchange limit [9], [10]. Despite that, the above cryptographic accomplishments are not appropriate for encoding compacted images and their ciphertext can't be packed either, as the repetition of the plaintext has been expelled in the encryption strategy [11], [12]. The execution of the various optimization algorithms utilized as a part of cryptographic methods additionally analyzed. A portion of the proposed strategies incorporates Ant Colony Optimization (ACO) based Cryptographic procedures; Genetic Algorithm (GA) based key trade, Binary Particle Swarm Optimization (BPSO) for image strategy and so forth [13]. To recognize an ideal security level, the cost of the sight and sound data to ensure and the cost of the assurance itself are looking at precisely [14]. Then again, image decryption recovers the first image from the encoded one. There are different image encryption frameworks to encode and decrypt information, and there is no single encryption algorithm fulfills the diverse image types [15].

2. Literature review

In 2017, Junxin Chen et al. [16] have proposed the essential presented systems are Compressed Sensing (CS) utilizing Structurally Random Matrix (SRM), and stage dissemination type image encryption. The encryption implementation starts from both the procedures; though the pressure impact accomplished by CS., 3-D cat map is utilized for key flow time. At the same time delivering three state factors of 3-D cat map utilized for the SRM age, image stage and dissemination. Numerical simulations and security examinations completed, and the outcomes show the adequacy and security execution of the proposed framework.

A large number of pictures are exchanged each day over the system by Laiphrakpam Dolendro Singh [17]. Some of these images are secret and they exchange the pictures safely. The exponentially difficult issue to settle an Elliptic Curve Discrete Logarithm Problem regarding the key size of Elliptic Curve Cryptography helps in furnishing an abnormal state of security with littler key size contrasted with other cryptographic system, which relies upon whole number factorization or Discrete Logarithmic issue. It disregarded the utilization of reference mapping table for encryption and decoding.

The author (Mohamed Elhoseny et al. 2016) [18] have proposed encryption key is 176- bit and is created by consolidating the ECC key, hub ID number, and separation to its Cluster Head (CH). To diminish energy utilization of CH, homomorphic encryption is utilized to enable CH to total the encrypted information without decrypting them. The demonstrated strategy was able to effort with various detecting situations that requirecatching content information and in addition images. Contrasted and the cutting edge strategies, our experimental outcomes showed that our proposed strategy enormously enhance the system execution as far as lifetime, communication overhead, memory prerequisites, and energy utilization.

Changing over data (information) from its unique shape to another frame is referred to as encryption as consecutively rising the data assurance by Mohamed A. Mokhtar et al. in 2017 [19]. The first image split into blocks and afterward unique chaotic maps utilized for five phases of proposed encryption calculation. To begin with, the cubic map utilized to permute the pixels, which contained inside the squares. Second, Henondelineates to diffuse the permuted pixels. Third, a quadratic guide attempted to permute the pieces. Fourth, a calculated guide used to permute every one of the pixels whole an image. At last, XOR Henon delineates to diffuse the permuted image.

In 2015, SeyedaliMirjalili et al. [20] The ALO calculation copies the chasing component of antlions in nature. Five principle ventures of chasing prey, for example, the irregular stroll of ants, building traps, entanglement of ants in traps, discovering preys, and re-building traps were actualized. Finally, the states of two ship propellers were enhanced by ALO as trying obliged genuine issues. In the initial two test stages, the ALO calculation was contrasted and an assortment of calculations in the writing. The consequences of the test functions demonstrated that the proposed calculation could give extremely focused outcomes as far as the enhanced investigation, nearby optima evasion, misuse, and meeting. The ALO calculation additionally discovers unrivaled ideal plans for the lion's share of established designing issues utilized, demonstrating that this calculation has justified in taking care of compelled issues with different pursuit spaces.

3. Existing problem for image security

- In the earlier decades, examine about in security has concentrated on the change of algorithms and traditions for encryption, verification, and decency of textual data or data with relative attributes image.
- These existing security systems are also using encryption or steganography, or their mixes. There is distinctive securable and perfect course of action of image encryption that can be all around protected from unapproved contact.
- Some of the presented researchers titled as public key image encryption are not affect a public key cryptosystem to scramble an image. They use a symmetric cryptosystem to scramble the image and an open key cryptosystem essentially associated as a key exchange tradition.
- One of the fundamental disadvantages of ECC is that it expands the span of the encrypted message significantly more than RSA encryption.

4. Methodology

Image encryption procedures have been progressively concentrated to support the demand for real-time secure image transmission over world. Encryption is the process of transforming the data for its security. Our proposed model (figure 1) used to secure the images with the help of encryption strategy; for this situation considers the images to apply histogram equalization to the removal of noise. Separated pixel values of images made for the secure image transmission and keep up the image data privacy, and after that, the image shares are isolated into blocks. The fundamental idea is that an image can be seen as a plan of blocks. The coherent data show in an image is because of the connection among the image components in a given model. Nevertheless, the image encryption and decryption process Homomorphic Encryption (HE) procedure are used.

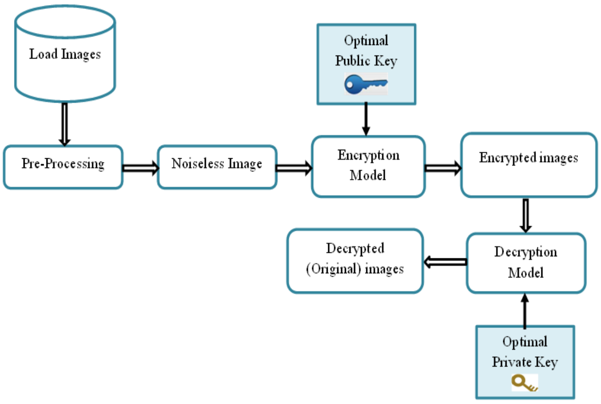


Fig. 1: Block Diagram for Proposed Model.

Moreover, encryption allows transmission and storage of secret images; it requires extraction in the way of secret key. In the encryption process, the public key arbitrarily created and the decryption procedure utilizes the optimization method for the private key generation of the HE procedure help of Ant Lion Optimization (ALO). The execution of the image is taken as fitness value for the optimization as expanding its entropy value. This ideal Homomorphic encryption in giving an effective security to the unique image; we propose an algorithm to perform encryption and decryption on images.

4.1. Preprocessing: histogram equalization

In the pre-processing stage histogram equalization plays an important role in our work. This is necessary when the image is transformed into new image the gray probability distribution is uniform during gray transformation [21]. This model achieves this task proficiently by distribution out the most continuous intensity values. After this stage, the image pixels are engaged as uniform gray level. Subsequently, the upgraded image has high complexity and extensive power range.

4.1.1. Image conversion

The pixel estimations of secret color image are removed and take as RGB pixel values and these qualities are independently shown as matrix the size of the matrix. Grayscale images have numerous shades of gray in the middle. Grayscale images are likewise called as monochromatic, signifying the nearness of just a single shading image. Subsequently, there are 0 to 255 power levels are there. Regardless of what pixel depth is utilized, the binary representations accept that zero is black and the extreme value is white, if not generally noted. A similar size of the first pixel estimations of the image is

$$Pixel = \sum R + G + B$$

Each pixel from the secret image is encrypted into different subpixels in each shared image utilizing a matrix to decide the shade of the pixels.

4.2. Homomorphic encryption

For encrypt the data or image, homomorphic encryption plays an extra operation which is denoted as a public key cryptosystem. This procedure has four functions, which are a Key generation, Encryption, Evaluation, and decryption, additionally, decrypt the information of evaluation algorithm; it provides an identical outcome if we had completed the operation on the first messages [22]. The decision of the plan is subject to the sort of operations being completed in the applications separated from different variables accustomed to pick the encryption plot.

4.2.1. Key generation

A technique for encoding and decoding keys and the related image utilizing a symmetric key; both secrecy and trustworthiness security is given. A private key and its relating public key; a key match is utilized with an asymmetric key (public-key) algorithm. Presently key Generation algorithm continues to pick the extra parameters to register the public key and private Key.

$$(H_{pk\ and}\ H_{sk})$$

$$K = cd \ \ and \ \ \omega = lcm(r-1, s-1)$$

For this procedure generate random keys for encryption and decryption , while optimization this keys utilizing ALO strategy and getting ideal private and public key do the rest of the system of image security forms.

4.3. Ant lion optimization (ALO)

ALO is a freshly proposed innovative optimization algorithm that was invented by Mirjilili. This algorithm inspired from hunting procedure of antlions in nature. This algorithm comprises of an investigation by irregular walk and arbitrary choice of specialists. The exploitation is finished with traps. It principally utilizes five fundamental strides of chasing i.e. arbitrary stroll of specialists, building traps, ensnarement of ants in a trap, getting prey and reconstructing traps. The roulette wheel strolls of ants in ALO optimizer agent can dispense with neighborhood optima.

4.3.1. Random walk of ants (keys for encryption, decryption process)

Ants, travel around the search space utilizing distinctive random walks, the traps of antlions influence Random walks and the Antlions can assemble openings corresponding to their fitness.

$$K_{keys} = \{\alpha_{k1}, \alpha_{k2}, \alpha_{k3}, ...\alpha_{kn}\}$$

Every ant can be gotten by an antlion in every iteration and the first class (fittest antlion). The scope of the arbitrary walk is diminished adaptively to reproduce down ants towards antlions.

4.3.2. Fitness (entropy)

Entropy is a scalar value representing to the entropy of grayscale image. Entropy is a factual measure of haphazardness that can be utilized to portray the surface of the info image. Image having most noteworthy entropy and least correlation coefficient is chosen as best cipher image and afterward, this image is sent to the goal.

$$Fitness = MAX\ (Entropy)$$

$$Entropy = \sum_{i=0}^{2N-1} P_i \log(1/P_i)$$

Fitness computation process in every generation, the individuals that are not chosen as elites do not take an interest in reproduction amid the whole algorithm, regardless of the way that their mix with the elites may bring about better solutions.
Here

$$N \square\ Number\ of\ \ gray\ \ level$$

$$P_i \square\ \mathrm{Pr}oability\ \ of\ \ i^{th} graylevel\ \ image$$

4.3.3. New ant lion (keys) updating

To reproduce such communications, ants are imperative to shift above the interest space and antlions are permissible to pursue them and twist up discernibly fitter using traps. Random walks of antlions are introduced in view of the underneath condition.

$$Opt\_key = \{0, cs(2r(t_1 \square 1)), cs(2r(t_2 \square 1))....................cs(2r(t_n \square 1))\}$$

$$r(t) = \begin{cases} 1 \ \ if \ \ rand > 0.5 \\ 0 \ \ if \ \ rand \le 0.5 \end{cases}$$

Where

$$cs \square\ Cumlative\ \ sum$$

$$n \square\ Max\ \ Number\ of\ \ \ Iteration$$

$$r(t) \square\ Stochanstic\ \ function$$

Nevertheless, above condition can't be straightforwardly utilized for updating the position of ants. With a specific end goal to keep the arbitrary strolls inside the pursuit space, they are standardized utilizing Min-Max Normalization process.

$$K,n(t) = \frac{\left(K_i^t - \min(k_i^t)\right) * \left(U(t) - L(t)\right)}{\left(\max(k_i^t - \min(k_i^t)\right)}$$

It defines the minimum and maximum of a random walk for the variable of n^{th} ant, $U(t)$ and $L(t)$ is the upper and lower bounds of d^{th} variable at t^{th} iteration.

4.3.4. Antlion building traps

The higher probability of catching ants is represented as a greatest fitness. In here, the arbitrary walk of ant isleaded by the chosen antlion and the first class ant lion and consequently, the relocation of a specifiedant appears as normal of both the irregular walks [23].

$$K,n(t)elite = \frac{R_k(t) + R_E(t)}{2}$$

Where R_k (t) a random is walk around ant lion K_{sel} and R_E(t) is the random walk around elite antlion K_{elite}

4.3.4. Catching ants and rebuilding pits

At the point when the fitness estimation of the key (ant) is better (max) than the fitness of antlion, at that point antlion gets the ant and after that updates its position to the ants' position as characterized beneath:

$$\chi_{AL,j}(t) = \chi_{A,i}(t) \ \ if \ \ f(\chi_{A,i}(t)) < f(\chi_{AL,j}(t))$$

This process is obtained by concatenating all fitness value and sorts them from smallest to largest fitness.

$$K_{optimal} = K_i(t) \ \ if \ \ f(K_i(t)) < f(K_n(t))$$

Given that the elite are the fittest antlion, it should have the ability to influence the advancements of the extensive number of ants in the midst of iterations. At that point, first N lines are updated as Antlion fitness and the relating position of antlions that is ideal keys.

4.4. Optimal key based encryption

An Encryption algorithm is currently functional to the secret image of the first image. In encryption process review the ideal public key has to encode each pixel of an image. It can be considered as message bit m, calculate the figure inform cipher data action.
Using secret key H_{sk} client encrypt the original image I_p and generate $H_{k\text{-}opt}(I_p)$ and along with the public key, K_{pk} this cipher image I_c will be sent to the server. $H_{pk} = (k, i)$ and $K_{sk} = (c, d)$ $Enc(I, H_{sk})$ for choose random variable $\square\, r \square\, Z_k^*$, Compute cipher data $c = I.r^k \bmod k^2$

4.5. Decryption

In the decryption procedure, review the image cipher which comprises of encrypted pixel spoke to by (c, d) and the Secret vector s. The decryption process is included with the utilization of two veils, in particular, the secret mask <as> and the even Masks in a steady progression. To decode the message bit (pixel esteem) m from the ciphertext and other secret parameters. Created $dec(f\,(H_{sk\text{-}opt}))$ will be decrypted by the customer utilizing its K_s and it gets the first outcome. This HE procedure for image security graphical portrayal appears in figure 2.

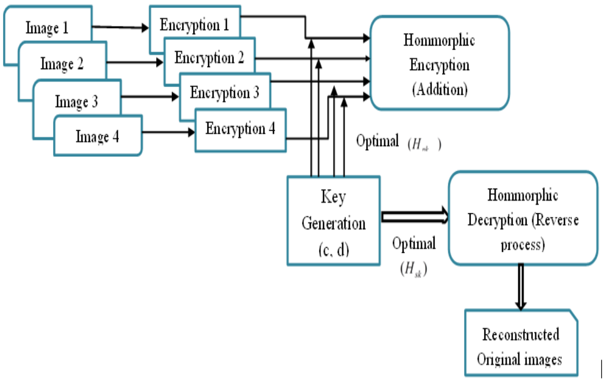


Fig. 2: Homomorphic Encryption Model.

$$Dec\ \mathrm{Im}age = \frac{L(c^{\alpha} \bmod k_{opti}{}^{2})}{L(i^{\alpha} \bmod k_{opt}{}^{2})} \bmod k$$

4.6. Evaluation

Homomorphic operations such as Addition and Multiplications can be executed on the encoded image will deliver the new encrypted image whose decryption will provide the yield with the similar functionality. The homomorphic operation can be connected to the comparing pixels of two encoded images. Give utilize a chance to consider the two relating pixels from two encoded images $C1 = <c1, d1>$ *and* $C2 = <c2, d2>$ .Addition operation on the ciphertext $C1$ and $C2$ is direct: including the comparing components of u terms and v terms create the new cipher image.
Steps for the Proposed Method
Input

- Load Secret image

Preprocessing

- Histogram equalization and RGB to gray conversion
- Image Security
- Homomorphic Encryption
- Key generation using ALO procedure
- Fitness as Entropy
- Get the Entropy of plain Image
- If optimal key {MAX entropy}
- Encryption based on optimal $(optimal\text{-}H_{pk\ and\ H_{sk}})$
- Decryption using optimal private key

5. Result and discussion

Image security demonstrates with optimal key based HE has been executed utilizing MATLAB 2016a with an i5 processor and 4GB RAM. The simulation model is considering as four standard images (Lena, house, pepper, and monkey) with better determination. The anticipated image encryption plot is analyzed by methods for the security measure, for example, entropy, PSNR, MSE, and CC this segment talked about the consequences of proposed and existing image encryption approaches.

5.1. Experimental results

Table 1 shows the input and enhancement images. In the first row illustrates the original image and then the second row depicts the histogram for that original image. Finally, these grayscale features are added to improve the encryption form it is shown in the last row.

Table 1: Input and Enhancement Images

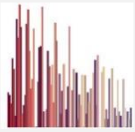
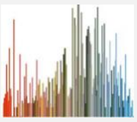
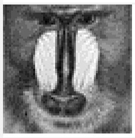
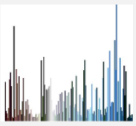
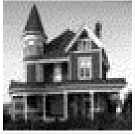
Images	Original Image	Histogram	Contrast Enhanced Gray image
Lena			
baboon			
pepper			
house			

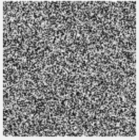
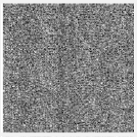
Table 2 depicts the proposed result for image security. For the respective four standard images, the performance i.e. PSNR, CC, MSE and entropy is analysed [24], [25], [26]. For example, Baboon gets the PSNR value as 52. 22, CC as 0.97, MSE reaches 0.21 and entropy achieve 7.85. Similarly, other images also attain the same type of result with respect to HE.

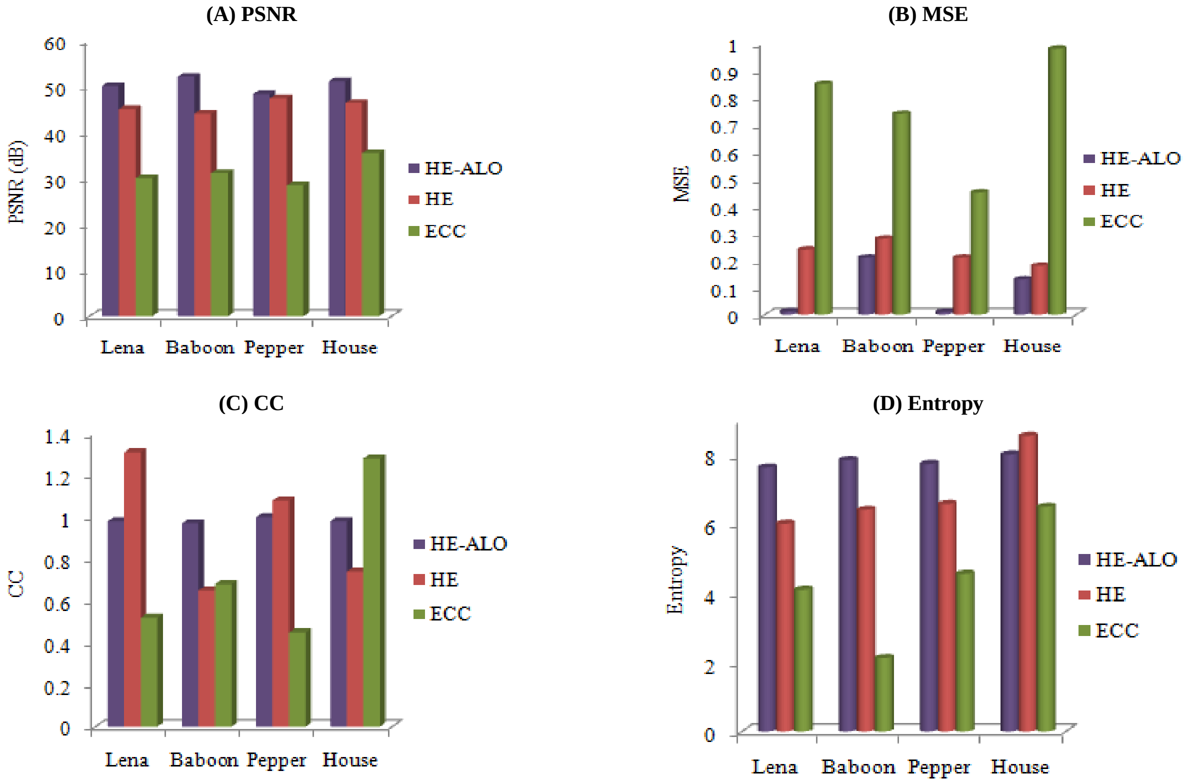
Table 2: Proposed (Optimal HE) Results for Image Security

Images	PSNR	CC	MSE	Entropy
Lena	50.21	0.98	0.012	7.64
Baboon	52.22	0.97	0.21	7.85
Pepper	48.45	1	0.01	7.74
House	51.22	0.98	0.13	8.012

Table 3 clarifies the performance analysis of standard images. The table examines the entropy and PSNR in view of encryption and decryption arrangement. The primary image gets the entropy as 7.64 and PSNR as 50.21, for each image, the entropy value has been changed as for image and decrypted model. The high entropy comes to the in-house image as 8.012.

Table 3: Performance Analysis

Original Images	Encrypted Images	Decrypted Images	Decrypted Color Images	PSNR	Entropy
				50.21	7.64
				52.22	7.85
				48.45	7.74
				51.22	8.012



(A) PSNR

(B) MSE

(C) CC

(D) Entropy

Fig. 3: Comparative Analysis.

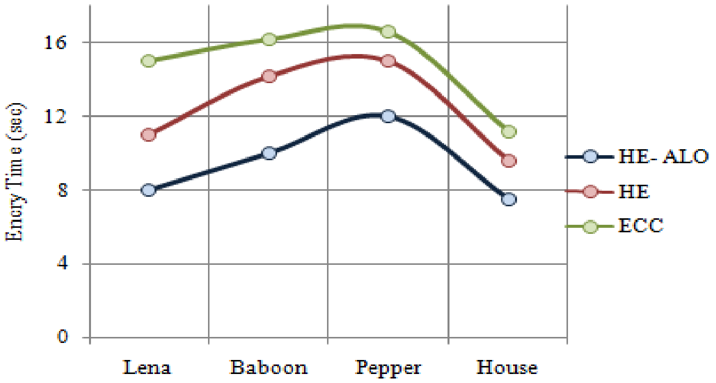


Fig. 4: Encryption Time Analysis.

Figure 4 delineates the encryption time analysis for standard images. The optimization procedure HE-ALO reduces the encryption time contrasted with HE and ECC. For example, in Leena image the time is taken for encryption in HE-ALO as 8 seconds, HE as 11 seconds, ECC achieves 15 seconds. In view of this correlation, proposed strategy achieves the optimal value.

6. Conclusion

The paper proposed a model for investigating digital Image processing operations on the encrypted images by adopting optimal key based Homomorphic Encryption. A proficient encryption algorithm that fulfills the HE to perform encryption and decryption on every one of the images is proposed. Here the decryption procedure is utilized with the assistance of Ant Lion Optimization (ALO) algorithm. The investigational examination is finished by performing a key examination, histogram investigation; PSNR, MSE examination, entropy and the outcome are clarified in detail. The investigation strategies are contrasted and the existing systems i.e. HE and ECC by applying the proposed algorithm (HE-ALO) to the standard images. The fitness function as entropy is inspected ideally in proposed strategy for all the standard images. The execution of the proposed technique is investigated regarding eliminating the communication time. In future, we will concentrate on new inspired algorithms to enhance the execution of the homomorphic encryption. Enduring and future progression in cryptography procedures, such as, that on dynamic completely homomorphic encryption and lightweight secure correlation conventions, will be basic in making the cryptography based approach more useful for the utilization of content-based image recovery.

References

[1] Chen, J., Zhang, Y., Qi, L., Fu, C. and Xu, L., "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression." *Optics & Laser Technology*, Vol. 99, pp.238-248. 2018. https://doi.org/10.1016/j.optlastec.2017.09.008.

[2] Ping, P., Xu, F., Mao, Y. and Wang, Z., "Designing permutation-substitution image encryption networks with Henon map". *Neurocomputing*, pp.1-17. 2017.

[3] Han, C., Shen, Y. and Ma, W. Iteration and superposition encryption scheme for image sequences based on multi-dimensional keys. *Optics Communications*, Vol. 405, pp.101-106.2017.

[4] Challa, R., Vijayakumar, G. and Sunny, B., "Secure Image processing using LWE based Homomorphic encryption". *In Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference* on pp. 1-6. IEEE.2015. https://doi.org/10.1109/ICECCT.2015.7226064.

[5] Meneses, F., Fuertes, W., Sancho, J., Salvador, S., Flores, D., Aules, H., Castro, F., Torres, J., Miranda, A.,and Nuela, D.,. *RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages*. International Journal of Computer Science and Network Security (IJCSNS), Vol.16, No.8, pp.55-62. 2016.

[6] Kumari, A. and Goyal, S., "Encryption and Code Breaking of Image Using Genetic Algorithm in MATLAB". *International Journal of Advance Research in Computer Science and Management Studies*, Vol.4, No.7, pp.356-361.2016.

[7] Kaushal, S., Thada, V. and Jatain, M.A., "Effect of Optimization Algorithm on Image Security and Reliability". *Journal of Advanced Research in Computer Engineering & Technology*, Vol.5, No.5, pp.1475-1478. 2016.

[8] Palvi Gupta, and Ridhi Kapoor, "Image Security using Optimized AES with GA", *Journal of Advances in Science and Technology*, Vol.3, No.3, pp.56-61.2015.

[9] Sayiema Amin, Durfi Ashraf and Amardeep Singh Virk, "Optimization of Steganography Technique using AES", *Journal of Innovative Research in Science, Engineering, and Technology*, Vol.4, No.8, pp.7498-7505. 2015.

[10] Praveenkumar,P. Devi,S. Thenmozhi,. Rayappan and Amirtharajan, R., "Stego integrated Image encryption using row and column indexing", *Conference on Computer Communication and Informatics*, pp.1-4. 2017.

[11] Reddy.V, and Siddaiah.P. "Genetic Algorithm Optimized Multi-Objective Optimization for Medical Image Watermarking using DWT and SVD", *Journal of Scientific & Engineering Research*, Vol.6, No.1, pp.1467-1479. 2015.

[12] Sindhuja, K. and Devi, P.S., "A symmetric key encryption technique using a genetic algorithm". *International Journal of Computer Science and Information Technologies*, Vol.5, No.1, pp.414-416. 2014.

[13] Pandey, L.N.,and Shukla, N.,. "Visual cryptography schemes using compressed random shares". *International Journal of Advance Research in Computer Science and Management Studies*, Vol.1, No.4, pp.62-66, 2013.

[14] Sasi, S.B. and Sivanandam, N., "A survey on cryptography using optimization algorithms in WSNs". *Indian Journal of Science and Technology*, Vol.8, No.3, pp. 216-221. 2015. https://doi.org/10.17485/ijst/2015/v8i3/59585.

[15] Yuan, S., Yang, Y., Liu, X., Zhou, X. and Wei, Z., "Optical image transformation and encryption by phase-retrieval-based double random-phase encoding and compressive ghost imaging". *Optics and Lasers in Engineering*, Vol.100, pp.105-110. 2018. https://doi.org/10.1016/j.optlaseng.2017.07.015.

[16] Chen, J., Zhang, Y., Qi, L., Fu, C. and Xu, L., "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression". *Optics & Laser Technology*, Vol.99, pp.238-248.2018.

[17] Singh, L.D., and Singh, K.M., "Image encryption using elliptic curve cryptography". *Procedia Computer Science*, Vol.54, pp.472-481. 2015. https://doi.org/10.1016/j.procs.2015.06.054.

[18] Elhoseny, M., Elminir, H., Riad, A. and Yuan, X.,. "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption". *Journal of King Saud University-Computer and Information Sciences*, Vol. 28, No.3, pp.262-275, 2016. https://doi.org/10.1016/j.jksuci.2015.11.001.

[19] Mokhtar, M.A., Sadek, N.M. and Mohamed, A.G. Design of image encryption algorithm based on the different chaotic mapping. *In Radio Science Conference (NRSC), 2017 34th National* pp. 197-204. IEEE. 2017. https://doi.org/10.1109/NRSC.2017.7893504.

[20] Mirjalili, S. "The ant lion optimizer". *Advances in Engineering Software*, Vol.83, pp.80-98. 2015. https://doi.org/10.1016/j.advengsoft.2015.01.010.

[21] Singh, R.P., and Dixit, M. "Histogram equalization: a strong technique for image enhancement". *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol.8, No.8, pp.345-352.2015.

[22] Zheng, P. and Huang, J. "An efficient image homomorphic encryption scheme with small ciphertext expansion". *In Proceedings of the 21st ACM international conference on Multimedia*, pp. 803-812. ACM. 2013. https://doi.org/10.1145/2502081.2502105.

[23] Mostafa, A., Houseni, M., Allam, N., Hassanien, A.E., Hefny, H. and Tsai, P.W. "Antlion Optimization Based Segmentation for MRI Liver Images". *In International Conference on Genetic and Evolutionary Computing*, Springer, pp. 265-272. 2016.

[24] Shankar, K., and P. Eswaran. "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography." China Communications 14.2 (2017): 118-130. https://doi.org/10.1109/CC.2017.7868160.

[25] Shankar, K., and P. Eswaran. "Sharing a secret image with encapsulated shares in visual cryptography." Procedia Computer Science 70 (2015): 462-468. https://doi.org/10.1016/j.procs.2015.10.080.

[26] Shankar, K., and P. Eswaran. "A new k out of n secret image sharing scheme in visual cryptography." Intelligent Systems and Control (ISCO), 2016 10th International Conference on. IEEE, 2016. https://doi.org/10.1109/ISCO.2016.7726969.