applied sciences

MDPI

Article

Optimal Multikey Homomorphic Encryption with Steganography Approach for Multimedia Security in Internet of Everything Environment

Ibrahim Abunadi [1], Hanan Abdullah Mengash [2], Saud S. Alotaibi [3], Mashael M. Asiri [4], Manar Ahmed Hamza [5,*], Abu Sarwar Zamani [5], Abdelwahed Motwakel [5] and Ishfaq Yaseen [5]

1 Department of Information Systems, College of Computer and Information Sciences, Prince Sultan University, Riyadh 12435, Saudi Arabia; iabunadi@psu.edu.sa
2 Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; hmengash@pnu.edu.sa
3 Department of Information Systems, College of Computing and Information System, Umm Al-Qura University, Mecca 24382, Saudi Arabia; sotaibi@uqu.edu.sa
4 Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Abha 62529, Saudi Arabia; abushrara@kku.edu.sa
5 Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia; zamani@psau.edu.sa (A.S.Z.); asmaeil@psau.edu.sa (A.M.); iyaseen@psau.edu.sa (I.Y.)
* Correspondence: ma.hamza@psau.edu.sa

Abstract: Recent developments of semiconductor and communication technologies have resulted in the interconnection of numerous devices in offering seamless communication and services, which is termed as Internet of Everything (IoE). It is a subset of Internet of Things (IoT) which finds helpful in several applications namely smart city, smart home, precise agriculture, healthcare, logistics, etc. Despite the benefits of IoE, it is limited to processing and storage abilities, resulting in the degradation of device safety, privacy, and efficiency. Security and privacy become major concerns in the transmission of multimedia data over the IoE network. Encryption and image steganography is considered effective solutions to accomplish secure data transmission in the IoE environment. For resolving the limitations of the existing works, this article proposes an optimal multikey homomorphic encryption with steganography approach for multimedia security (OMKHES-MS) technique in the IoE environment. Primarily, singular value decomposition (SVD) model is applied for the separation of cover images into RGB elements. Besides, optimum pixel selection process is carried out using coyote optimization algorithm (COA). At the same time, the encryption of secret images is performed using poor and rich optimization (PRO) with multikey homomorphic encryption (MKHE) technique. Finally, the cipher image is embedded into the chosen pixel values of the cover image to generate stego image. For assessing the better outcomes of the OMKHES-MS model, a wide range of experiments were carried out. The extensive comparative analysis reported the supremacy of the proposed model over the rennet approaches interms of different measures.

Keywords: internet of everything; multimedia data; security; privacy; encryption; image steganography; pixel selection

Citation: Abunadi, I.; Abdullah Mengash, H.; S. Alotaibi, S.; Asiri, M.M.; Ahmed Hamza, M.; Zamani, A.S.; Motwakel, A.; Yaseen, I. Optimal Multikey Homomorphic Encryption with Steganography Approach for Multimedia Security in Internet of Everything Environment. *Appl. Sci.* **2022**, *12*, 4026. https://doi.org/10.3390/app12084026

Academic Editor: Ki-Hyun Jung

Received: 19 February 2022
Accepted: 6 April 2022
Published: 15 April 2022

1. Introduction

Internet of Everything (IoE) represents a fantastic vision in the future, where everything is interconnected to the Internet, thus facilitating decision-making and offering intelligent service. IoE application based on interdisciplinary technological innovation includes low power communications, big data analytics, sensor, and embedded techniques [1]. Over the years, increasing new technologies are emerged to provide new bricks to construct IoE. Firstly, the advancement in sensor and embedded techniques have made the Internet of

Things (IoT) node being less energy consumption and more portable [2]. The IoT involves the interconnectivity of physical objects and data input and output, whereas the IoE is a comprehensive term that refers to the interconnectivity of various technologies, processes, and people. Next, the presence of Lower Power Wide Area Network (LPWAN) technology empowers the ubiquitous network connection of lower power IoT nodes [3]. Further, the availability of massive IoT data and the innovation in artificial intelligence have driven the intelligence of IoE. Thus, IoE is employed in wide-ranging applications like intelligent transportation systems, smart manufacturing, and smart agriculture. Figure 1 depicts the process of IoE.

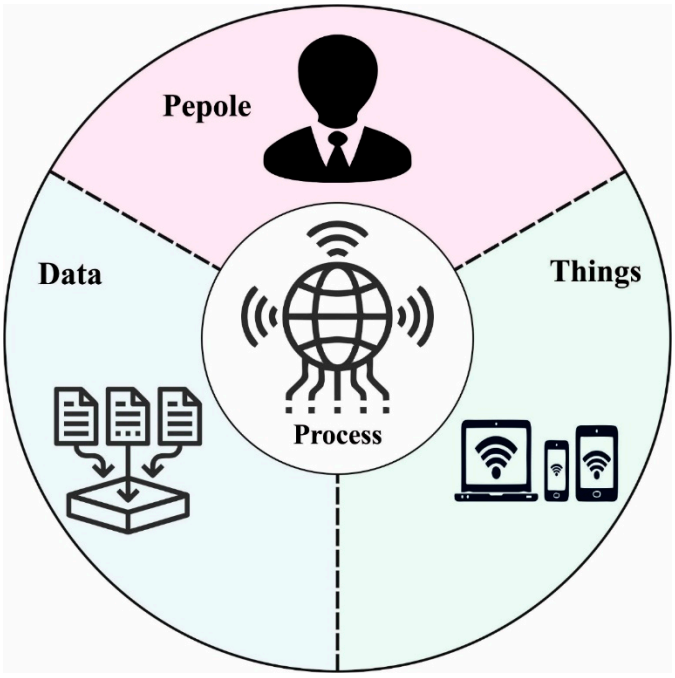

Figure 1. Representation of IoE.

Many possible security risks are experienced in IoE, attributed to the vulnerability of transmission protocol and resource limitation of IoE node [4]. Especially, the existing IoE mainly adopts the lower-cost and simplified access protocols for reducing cost of the network whereas it makes the communication vulnerable to malicious attacks like forging and eavesdropping. On the contrary, the data emitted from end node is eavesdropped (or wiretapped) by malicious node; at the same time, and pseudo-base-station could easily forge the standard IoE transmission connections to attain IoE data [5]. Thus, an efficient and easy-deployed security method is needed for protecting IoE communication from malicious attacks. Typically, encryption is utilized for ensuring data privacy and confidentiality, at the expense of utility (for example, searching on ciphertext becomes challenging and costly). Generally, Current encryption solution assumes that the cloud server is honest-but-curious, that implements search operation according to the agreed protocol however it might be interested in potentially learning sensitive data [6]. But in a real-time scenario the cloud server is highly possible to be semi-trusted in the sense that it never accessed or might delete rarely information to conduct partial search operation, output a fraction of inaccurate search results, cut costs (for example, minimizing computation overhead and storage space), etc. [7].

Steganography represents the fabrication technique that is utilized as digital information to the cover media. It provides security to the hidden and sensitive data existing in the image that is undetectable by human vision [8]. Still, several studies in this field are needed for selecting appropriate tradeoffs among the performance evaluations like payload capacity, security, and imperceptibility. Now, secure information is transmitted through text

messages, images, audio, and videos files. To transmit this message in a hidden method, there is necessity for steganography. In this approach, the embedded secret message in the file is transported to the user alternatively, whereby the message is unconcealed [9]. Even though there is much software accessible online for data security, there is another software that is in usage by hackers for decrypting the hidden information [10].

This article proposes an optimal multikey homomorphic encryption with steganography approach for multimedia security (OMKHES-MS) technique in the IoE environment. The OMKHES-MS model initially uses singular value decomposition (SVD) model. In addition, the optimal pixel points in the cover image are chosen by the use of coyote optimization algorithm (COA). Moreover, the encryption of secret images is performed using poor and rich optimization (PRO) with multikey homomorphic encryption techniques. Furthermore, the cipher image is embedded into the chosen pixel values of the cover image to generate stego image. To investigate the enhanced performance of the OMKHES-MS model, a comprehensive simulation analysis is performed and the results are investigated under several aspects.

2. Related Works

In [11], a machine learning (ML) based structure was presented for identifying benign and malicious nodes from an IoE network functioning with big data. A new technique to co-operate of extreme gradient boosting (XGBoost) and deep learning (DL) techniques together with genetic particle swarm optimization (GPSO) technique for discovering the optimum structures of individual ML techniques are presented. But the simulation, it can be demonstrated that GPSO based learning techniques offer reliable, robust, and scalable solutions. The authors in [12] analyzed the existing structures utilized to develop secure IoE with big data analytics. Big data is a group of data created in the sensor embedding from nearby physical objects. This data was utilized to analyze surrounding and development depending upon the inference. IoE utilizes this information to automation of electronic equipment from the surrounding environments.

Mohanty et al. [13] presented a novel blockchain structure named as PUFchain and presents a novel consensus technique named "Proof of physical unclonable functions (PUF)-Enabled Authentication" (PoP) to be utilized from PUFchain. The presented PoP is the PUF combined as to before presented Proof-of-Authentication (PoAh) consensus technique is named as "HardwareAssisted PoAh (HA-PoAh)". Miao et al. [14] introduced a fair and dynamic data sharing framework (FairDynDSF) from the multi-owner setting. Utilizing FairDynDSF, one is to verify the correctness of searching outcomes, dynamic update, attain fair arbitration, and multi-keyword search.

Singh et al. [15] proposed a secure structure Blockchain and Fog-based Architecture Network (BFAN) for IoE application from the smart city. The presented infrastructure secures sensitive information with Blockchain, encryption, and authentication. It supports the System-developer and Architect for deploying the application from smart city paradigm. The purpose of presented infrastructure is for reducing the latency and energy, and make sure enhanced security features with Blockchain technologies. Li et al. [16] presented a privacy-enhanced federated learning model for IoE. 2 processes that were executed in our systems such as local adaptive differential privacy (LADP) and randomized response (RR) processes. The RR was implemented for preventing the server from discovering if upgrades are gathered from all the rounds.

3. The Proposed Model

In this study, a new OMKHES-MS technique has been developed to accomplish security and privacy in the IoE environment. The OMKHES-MS model involves a series of processes namely SVD, COA based optimum pixel selection, MKHE based encryption, and PRO based key generation. Finally, the cipher image from the MKHE technique is embedded into the chosen pixel values of the cover image to generate stego image. The

design of PRO algorithm helps in choosing optimum keys for the generation of cipher images. Figure 2 demonstrates the overall process of OMKHES-MS technique.

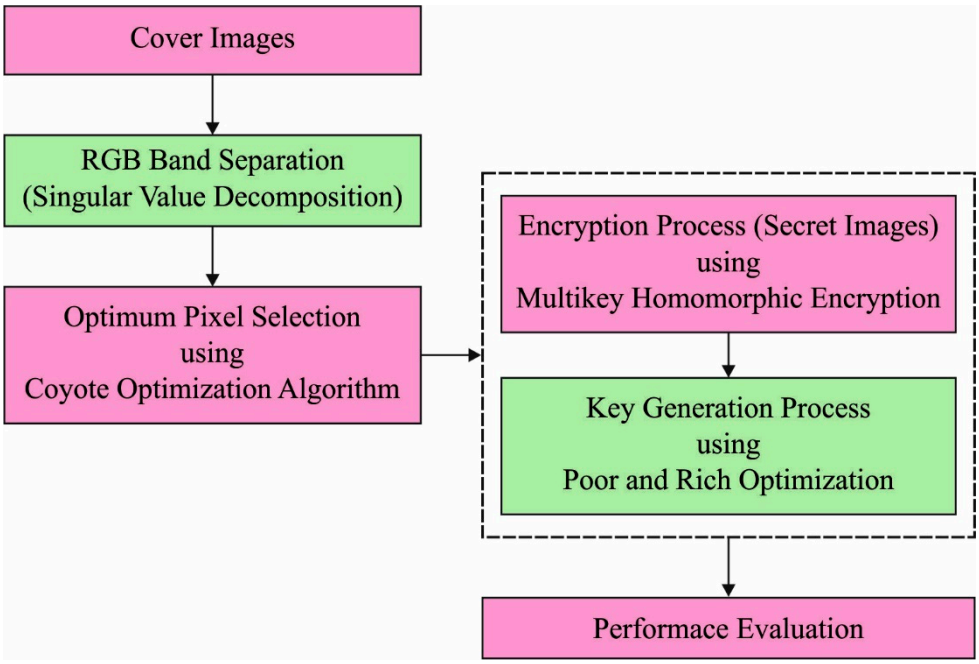

Figure 2. Overall process of OMKHES-MS technique.

3.1. Singular Value Decomposition

SVD is an influential tool that takes several applications like pattern detection and data compression. SVD allows robust and reliable matrix factorizes for extracting the algebraic and geometric invariant features of images. The SVD factorization a square/non-square matrices as to 2 orthogonal matrices and singular value (SV) matrix. The spatial domain feature of images of the size 100×100 is demonstrated utilizing SVD by feature vector group of size 1×100. It can be predictable for speeding up the computational procedure by removing irrelevant features but preserving as a lot of data as feasible from the images. The SVD of rectangular real complex matrix A has been formulated as follows [17].

$$A = U\Sigma V^T = \begin{bmatrix} u_{11} & \cdots & u_{1m} \\ u_{21} & \cdots & u_{2m} \\ \vdots & \ddots & \vdots \\ u_{m1} & \cdots & u_{mm} \end{bmatrix} \times \begin{bmatrix} s_1 & 0 & \cdots & 0 \\ 0 & s_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & s_m \end{bmatrix} \times \begin{bmatrix} v_{11} & \cdots & v_{1n} \\ v_{21} & \cdots & v_{2n} \\ \vdots & \ddots & \vdots \\ v_{n1} & \cdots & v_{nn} \end{bmatrix}_{n \times n}, \quad (1)$$

where

$$UU^T = I. \quad (2)$$

$$VV^T = I. \quad (3)$$

$$s_1 \geq s_2 \geq s_3 \ldots\ldots\ldots \geq s_m. \quad (4)$$

where A refers to the $m \times n$ matrices, U implies the $m \times m$ orthonormal matrices, V signifies the $n \times n$ orthonormal matrices, and Σ defines the diagonal matrices of sizes $m \times n$ that is collected of SVs of A such that it holds non-negative number.

The diagonal entry of Σ matrix signifies the SV and it can be superior values related to the entries of U and V so that matrix of size $m \times n$ is decreased to vector of sizes n. The SV is ranked in descending order; a primary entry of SV matrix contains the best substantial data but the final entry at the vector comprises the least significant data. The SV has the energy data but the orthogonal matrices contain the essential data. U^T and V^T are the transpose of matrices U and V correspondingly. I demonstrates the identity matrix. The

column of U is termed as left singular vector of A whereas the column of V is named as the right singular vector of A.

3.2. Optimal Pixel Selection Using COA

For selecting the pixel points in the cover image optimally, the COA is applied. A current metaheuristic method for global optimization named COA is adapted. The main concept is depending on canis latrans species that mostly exist in North America. The process is adopted for considering the social organization of the agent named coyotes that serves as an algorithmic construction. The social behavior of coyote serves as a design variable and it is determined in the following [18]:

$$soc_c^{p,t} = \overrightarrow{x} = (x_1,\ x_2,\ x_3,\ \ldots.,\ x_D). \tag{5}$$

This social condition includes adopting the coyote to the environment name $fit_c^{p,t} \in \Re$. The adaptation of the coyotes to the present social situation was evaluated by:

$$fit_c^{p,t} = f\left(soc_c^{p,t}\right). \tag{6}$$

Initially, the coyotes are arbitrarily allocated to the packs though the detail that they might leave sometimes their packs and developed solitary or affiliated to other packs. The coyote's transfer among packs increases the interaction of population with their culture. An alpha is selected from the three COA alphas:

$$alpha = \left\{ soc_c^{p,t} \middle| \underset{c=\{1,2,..Nc\}}{arg\ min} f\left(soc_c^{p,t}\right) \right\}. \tag{7}$$

With respect to the COA, it is assumed that each coyote has been ordered for exchanging the social culture. Thus, the present data of coyotes are interrelated and estimated as follows.

$$cult_j^{p,t} = \begin{cases} O^{p,t}_{\frac{(Nc+1)}{2}} & Nc\ is\ odd \\ \frac{o^{p,t}_{\frac{Nc}{2},j} + o^{pt}_{(\frac{Nc}{2}+1),j}}{2} & otherwise \end{cases}. \tag{8}$$

The social condition ranking of each coyote at t instant is offered by variable $O^{p,t}$. In another word, the median social condition of each coyote from that certain pack is applied for determining the cultural tendency. The birth of coyote represented as $age_c^{p,t}$, is a function of social grouping of two parents who are selected arbitrarily with regards to the effect of environment. Figure 3 demonstrates the flowchart of COA.

$$pup_j^{p,t} = \begin{cases} soc_{r1,j}^{p,t}\ rndj \prec P_s\ or\ j = j1 \\ soc_{r2,j}^{p,t}\ rndj \prec P_s + P_a\ or\ j = j2, \\ R_j\ otherwise \end{cases} \tag{9}$$

where $soc_{r1,j}^{p,t}$ and $soc_{r2,j}^{p,t}$ denotes the social condition of two coyotes r_1 and r_2 are randomly chosen and include the pth pack at time t. $j1$ and $j2$ denote the dimension of optimization problem that is chosen arbitrarily. P_s and P_a represents the possibility of scattering and the possibility of association, correspondingly. R_j is an arbitrarily created value in the range of variable bound. The cultural diversity of coyotes from the pack is performed by the two probabilities P_s and P_a, in the following:

$$P_s = \frac{1}{D}, \tag{10}$$

$$P_a = \frac{1 - P_s}{D}, \tag{11}$$

where D show the problem dimension inside the pack. The coyote under alpha effect δ_1 and pack effect δ_2, is defined in the following:

$$\delta_1 = alpha^{p,t} - soc_{cr2}^{p,t}, \tag{12}$$

$$\delta_2 = cult^{p,t} - soc_{cr2}^{p,t}, \tag{13}$$

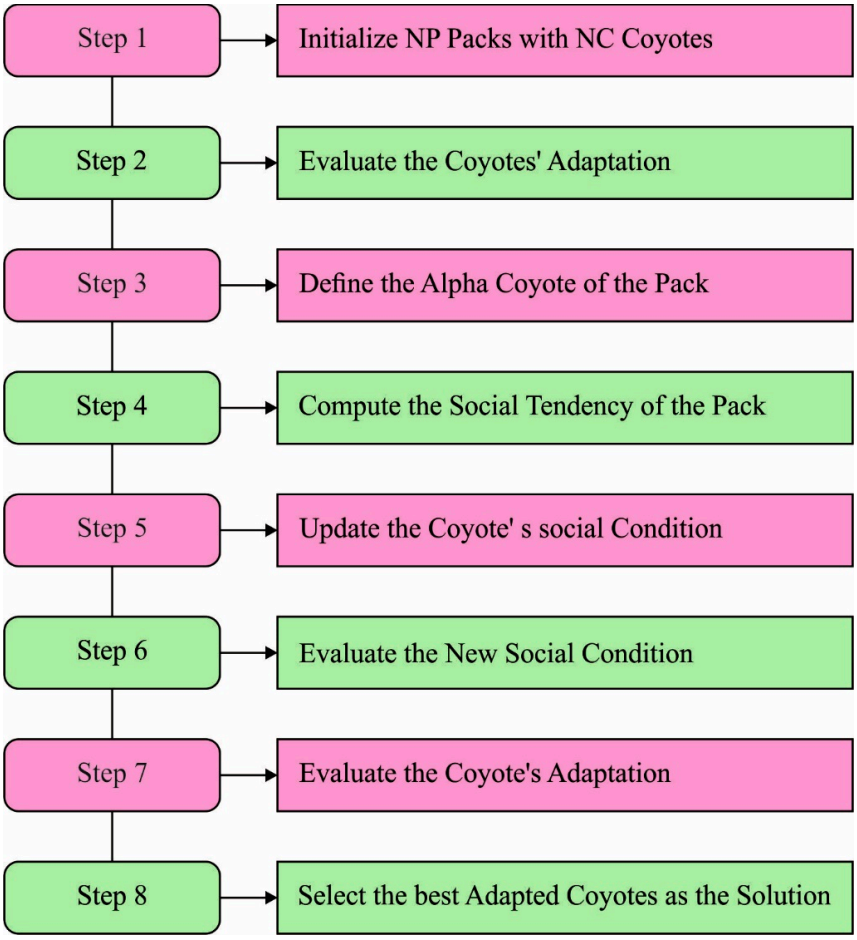

Figure 3. Flowchart of COA.

The alpha and pack effect remains significant parameter in the update of social coyote condition as follows:

$$soc_c^{p,t,new} = soc_c^{p,t,\,old} + r_1 \cdot \delta_1 + r_2 \cdot \delta_2, \tag{14}$$

The update procedure of the social condition can be accomplished by considering the subsequent condition:

$$soc_c^{p,t+1} = \begin{cases} soc_c^{p,t,new} \; fit_c^{p,t,new} \prec fit_c^{p,t} \\ soc_c^{p,t} \; otherwise \end{cases}, \tag{15}$$

3.3. Secret Image Encryption Using MKHE Technique

In order to effectually encrypt the secret image before steganography, the MKHE technique is applied. An MKHE is a cryptosystem that permits us for evaluating an arithmetic circuit on cipher-text, maybe encrypting in several keys. Assume that $\mathcal{M}$ remains the message space with arithmetic infrastructure [19]. An MKHE method has 5 PPT techniques (Eval, Setup, Enc, KeyGen, and Dec). It is considered that all contributing parties have a reference (index) to their public and confidential keys. A multi-key cipher-

text implicitly has an arranged set $T = \{id_1, \ldots, id_k\}$ of connected references. For instance, a fresh cipher-text $ct \leftarrow$MKHE. $Enc(\mu; pk_{id})$ equals to single-element set $T = \{id\}$ but the size of references fixed obtains superior to the computation amongst cipher-text in various party developments.

- Setup: $pp \leftarrow$ MKHE. $Setup(1^{\lambda})$. Proceeds the secured parameter as input and returned the public parameterization. It can be considered that every other technique implicitly gets pp as input.
- Key Generation: $(sk, pk) \leftarrow$ MKHE. $KeyGen(pp)$. Resultants a pair of confidential and public keys.
- Encryption: $ct \leftarrow$<KHE.$Enc(\mu; pk)$. Encrypting a plaintext $\mu \in \mathcal{M}$ and resultants a cipher-text $ct \in \{0,1\}^*$.
- Decryption: $\mu \leftarrow$MKHE. $Dec(\overline{ct}; \{sk_{id}\}_{id \in T})$. To provide a cipher-text $\overline{ct}$ with equivalent order of confidential keys, outcomes a plaintext μ.

The Homomorphic estimation is defined as follows:

$$\overline{ct} \leftarrow \text{MKHE.}Eva1(C, (\overline{ct}, \ldots, \overline{ct}_l), \{pk_{id}\}_{id \in T}). \tag{16}$$

To provide a circuit C, a tuple of multi-key cipher-text $(\overline{ct}, \ldots, \overline{ct}_l)$ and the equivalent group of public keys $\{pk_{id}\}_{id \in T}$, resultants a cipher-text $\overline{ct}$. Its reference set is union $T = T_1 \cup \cdots \cup T_\ell$ of reference sets T_j of input cipher-text $\overline{ct}_j$ for $1 \leq j \leq \ell$.

Semantic Security. To some 2 messages $\mu_0, \mu_1 \in \mathcal{M}$, the distribution {MKHE. Enc (μ_i; pk)} for $i = 0, 1$ can be computationally indistinguishable whereas $pp \leftarrow$MKHE. $Setup(1^{\lambda})$ and $(sk, pk) \leftarrow$MKHE. $KeyGen(pp)$. Correctness and Compactness. An MKHE technique was compact once the size of cipher-texts related to k parties is bounded by poly (λ, k) to set a polynomial poly $(\cdot\cdot)$. For $1 \leq j \leq \ell$, assume ct_j be cipher-text (with reference set T_j) so that MKHE. $Dec(\overline{ct}, \{sk_{id}\}_{id \in T_j}) = \mu_j$ Assume $C : \mathcal{M}^{\ell} \rightarrow \mathcal{M}$ be circuit and $\overline{ct} \leftarrow$ MKHE.$Eval(C, (\overline{ct}, \ldots, \overline{ct}), \{pk_{id}\}_{id \in T})$ for $T = T_1 \cup \cdots \cup T_\ell$. Afterward,

$$\text{MKHE. } Dec(\overline{ct}, \{sk_{id}\}_{id \in T}) = C(\mu_1, \ldots, \mu_\ell). \tag{17}$$

The equality is replaced by estimated equality same as the Cheon, Kim, Kim and Song (CKKS) technique to estimate arithmetic [16].

3.4. Key Generation Using PRO Algorithm

For optimal key generation process, the PRO algorithm is applied, which depends on people's wealth behavior in the society. Generally, it is classified into two financial groups within a society. Initially, it comprises of wealthier person (wealth is greater when compared to average). Second, it comprises poor people (wealth is lesser when compared to average). Rich economical class people attempt to extend the class gap by observing them from poor economical groups. During the optimization problem, every solution from the Poor population moves towards the global optimum solution in the searching space by learning from the rich solution from the rich population [20].

Solution encoding

Here, each Solution or Person in the population is characterized as binary vector. The person χ is characterized as $\chi = [\eta_1, \eta_2, \eta_3, \ldots, \eta_n]$ whereas n indicates the amount of features in text corpus. Each location of the solution or person α is binary value. $\eta_j \in \{0, 1\}$, For instance, a solution or person determined as [0, 1, 0, 1, 0, 0, 1, 1, 1, 0] represents that the features or terms with index 2, 4, 7, 8 and 9 are chosen.

Initial population

The set of solutions from the present generation is named a population. The candidate solution in the population consists of the rich and poor economical solution or person.

Consider 'N' is the population size. We arbitrarily create 'N' solutions with arbitrary numbers within [0, 1]. Next, the digitization procedure is employed to every location of solution to convert real value to binary values as follows

$$\chi_{i,j} = \begin{cases} 1, \ \chi_{i,j} > rand \\ 0, \ otherwise \end{cases}, \tag{18}$$

where rand represents an arbitrary value among 0 and 1. The candidate solution in the population is ordered according to the objective function. The topmost part of the population is denoted as rich economic class of people and the bottom part of the population is represented as poor economic class of people.

$$POP_{Main} = POP_{rich} + POP_{poor}. \tag{19}$$

Fitness Function

The COA intends to derive an objective function depending upon the fitness function. The major intention of the COA is to design a novel image steganography technique with the minimization of error (MSE) and maximization of PNSR. It is evaluated as

$$F = \{min(MSE), \ max(PSNR)\}. \tag{20}$$

The desired minimized and maximized value is obtained by the use of the inspired Whale optimization technique.

Generating new solutions

The rich people move towards to rise the economic class gap by observing them from the poor economical group. The poor economical class people move towards to decrease the economic class gap by learning from the rich economical class for increasing the financial condition. The general behavior of rich and poor people can be utilized for generating a new solution.

$$\chi^{new} = \chi^{old}_{rich, \ i,j} + \alpha * \left[\chi^{old}_{rich,i,j}\right| - \chi^{old}_{poor,best,j}\Big]. \tag{21}$$

$$\chi^{new}_{poor,i,j} = \chi^{old}_{poor,i,j} + \alpha * \left[\left(\frac{\chi^{0}_{rich,best,j} + \chi^{0}_{rich,mean,j} + \chi^{0}_{rich,worst,j}}{3}\right) - \chi^{0}_{poor,i,j}\right]. \tag{22}$$

To improve the level of security, the optimal keys of the MKHE technique are generated by the use of PRO algorithm.

4. Experimental Validation

4.1. Implementation Data

This section validates the performance of the OMKHES-MS technique using benchmark test images. The results are assessed under distinct such as Peak Signal Noise Ratio (PSNR), Maximum Difference (MD), Mean Squared Error (MSE), Root Mean Square Error (RMSE), Normalized Cross-Correlation (NCC), Average Difference (AD), maximum difference (MD), Normalized absolute Error (NAE), and Structural Content (SC). For enhanced performance, the values of PSNR, SC, and NCC should be as high as possible whereas MSE, RMSE, AD, NAE, and MD should be as low as possible.

Figure 4 shows the sample set of benchmark images used as secret images and the respective image histograms are offered in Figure 5.

Figure 4. Sample set of Secret Images.

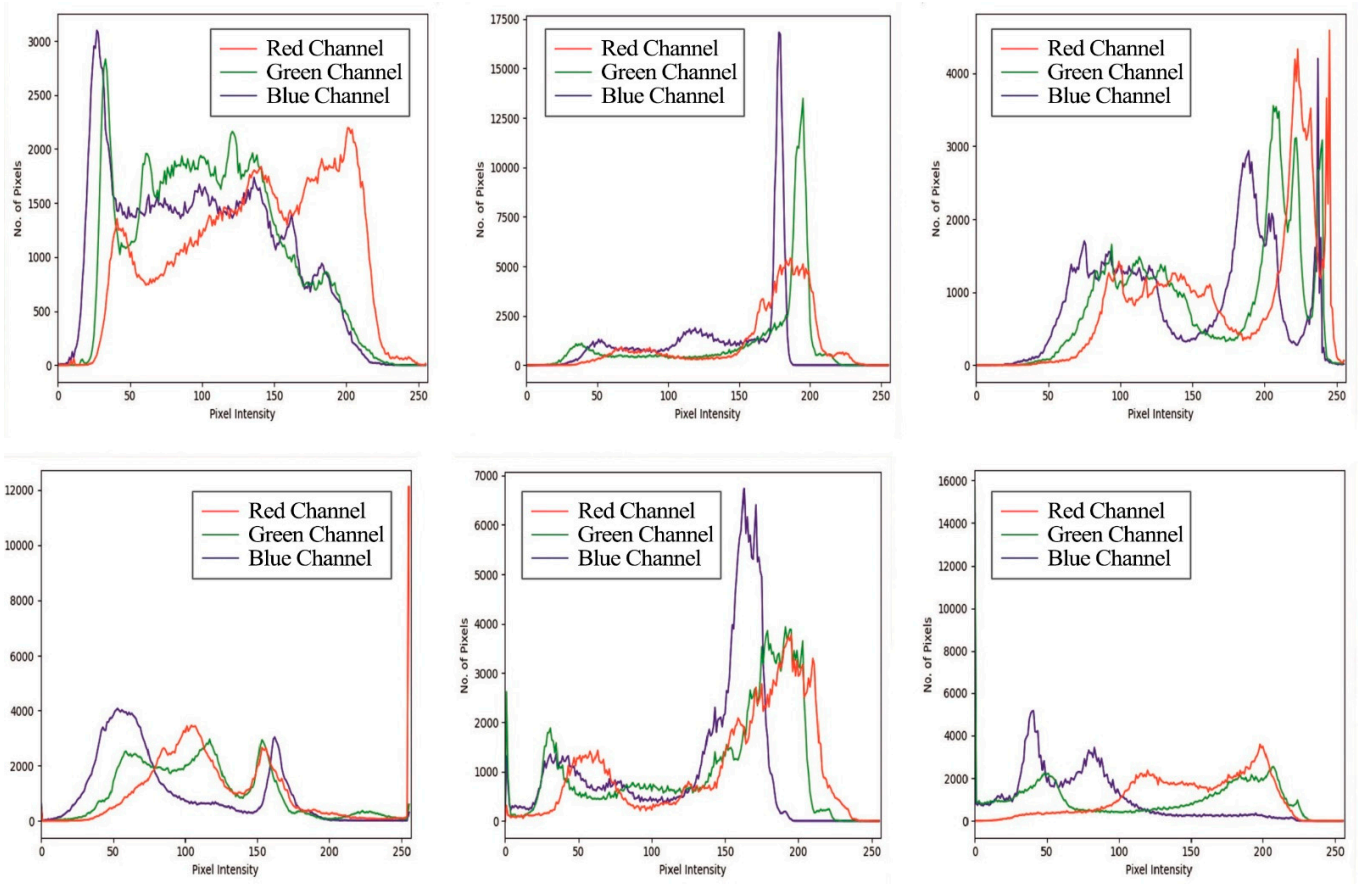

Figure 5. Histogram of Secret Images.

4.2. Discussion

Table 1 reports the MSE and RMSE examination of the OMKHES-MS model under distinct images. The experimental results indicated the improvements of the OMKHES-MS model interms of MSE and RMSE.

Table 1. MSE and RMSE analysis of OMKHES-MS technique with different images.

Images	MSE			RMSE		
	OMKHES-MS	WOA-EBS	GWO-EBS	OMKHES-MS	WOA-EBS	GWO-EBS
Barbara	0.2715	0.2840	0.5407	0.5211	0.5329	0.7353
Boat	0.3146	0.3447	0.8515	0.5609	0.5871	0.9228
Foreman	0.1703	0.1913	0.2732	0.4127	0.4374	0.5227
House	0.0595	0.0739	0.3037	0.2438	0.2718	0.5511
Isabe	0.3134	0.3478	0.6824	0.5598	0.5897	0.8261
Peppers	0.1937	0.2262	0.3053	0.4401	0.4756	0.5525

Figure 6 illustrates the MSE inspection of the OMKHES-MS model with existing models on distinct images. The results indicated that the OMKHES-MS model has offered effectual outcomes with minimal values of MSE over the other WOA-EBS and GWO-EBS models. For instance, with Barbara image, the OMKHES-MS model has obtained lower MSE of 0.2715 whereas the WOA-EBS and GWO-EBS models have offered higher MSE of 0.2840 and 0.5407 respectively. Followed by, with Peppers image, the OMKHES-MS model has gained reduced MSE of 0.1937 whereas the WOA-EBS and GWO-EBS models have provided increased MSE of 0.2262 and 0.3053 respectively.

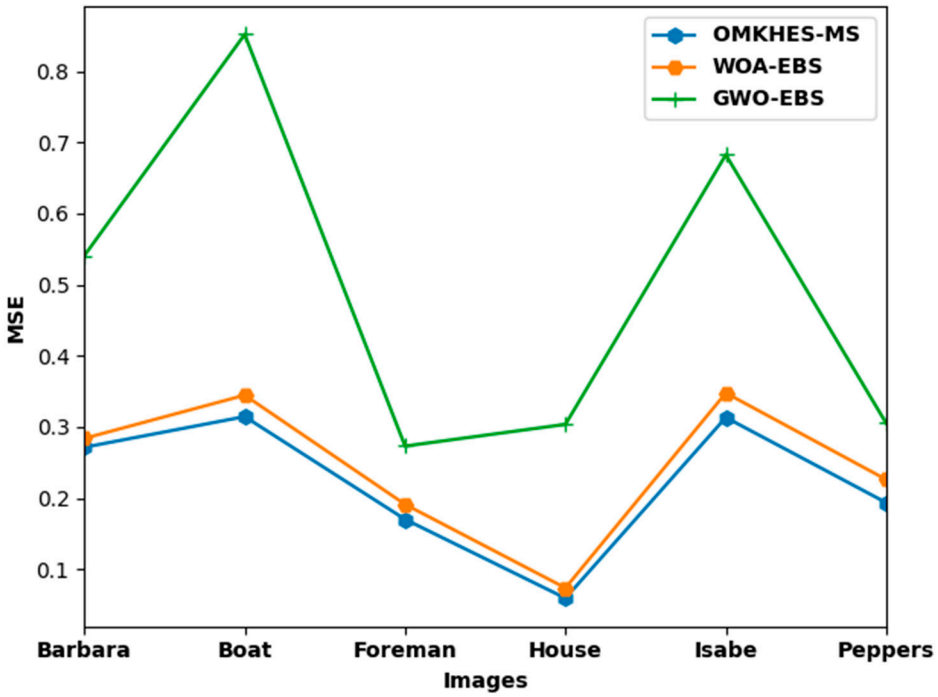

Figure 6. Comparative MSE analysis of OMKHES-MS technique with existing models.

Figure 7 exemplifies the RMSE examination of the OMKHES-MS model with existing models on diverse images. The experimental values reported that the OMKHES-MS model has resulted in improved performance with lower values of RMSE over the other WOA-EBS and GWO-EBS models. For instance, with Barbara image, the OMKHES-MS model has

attained decreased RMSE of 0.5211 whereas the WOA-EBS and GWO-EBS models have achieved increased RMSE of 0.5329 and 0.7353 respectively. In line with, Peppers image, the OMKHES-MS model has depicted minimal RMSE of 0.4401 whereas the WOA-EBS and GWO-EBS models have exhibited maximum RMSE of 0.4756 and 0.5525 respectively.

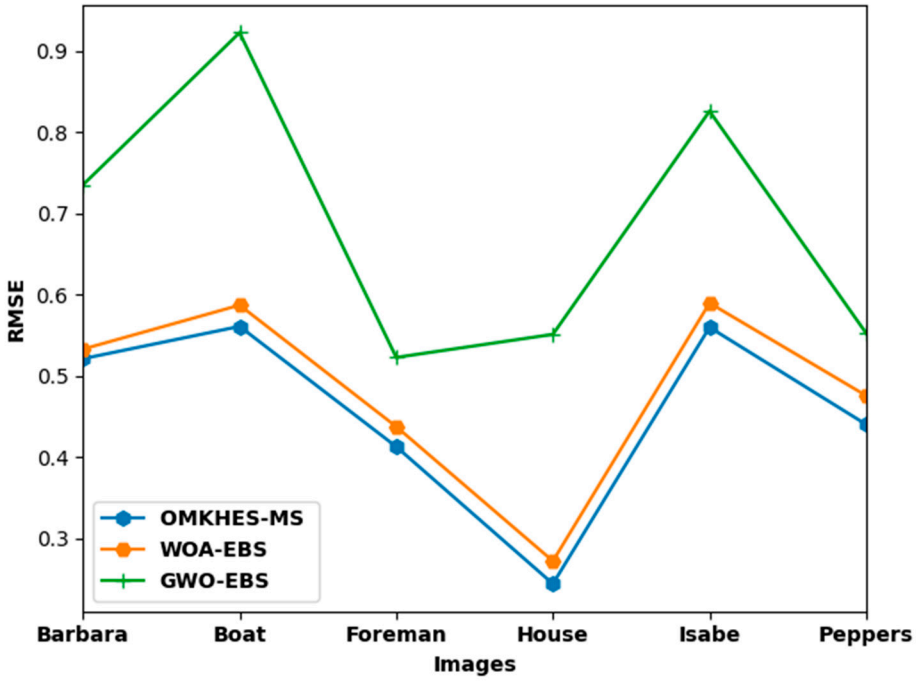

Figure 7. Comparative RMSE analysis of OMKHES-MS technique with existing models.

A comprehensive SC and PSNR assessment of the OMKHES-MS model is compared with recent methods in Table 2. The experimental values notified that the OMKHES-MS model has gained effectual outcome with maximum values of SC and PSNR. For instance, the OMKHES-MS model has offered higher SC of 0.9986, 0.9991, 0.9991, 0.9986, 0.9986, and 0.9987 on the test Barbara, Boat, Foreman, House, Isabe, and Peppers images respectively. At the same time, the OMKHES-MS model has provided increased PSNR of 59.4556 dB, 58.1759 dB, 63.5057 dB, 72.6470 dB, 58.2083 dB, and 62.3885 dB on the test Barbara, Boat, Foreman, House, Isabe, and Peppers images respectively.

Table 2. SC and PSNR analysis of OMKHES-MS technique with different images.

Images	Structural Content			Peak Signal Noise Ratio		
	OMKHES-MS	WOA-EBS	GWO-EBS	OMKHES-MS	WOA-EBS	GWO-EBS
Barbara	0.9986	0.9984	0.9984	59.4556	59.0647	53.4721
Boat	0.9991	0.9990	0.9989	58.1759	57.3818	49.5272
Foreman	0.9991	0.9990	0.9990	63.5057	62.4948	59.3999
House	0.9986	0.9984	0.9984	72.6470	70.7592	58.4823
Isabe	0.9986	0.9984	0.9985	58.2083	57.3049	51.4495
Peppers	0.9987	0.9984	0.9985	62.3885	61.0412	58.4367

A comparative SC analysis of the OMKHES-MS model with existing techniques under distinct test images is performed in Figure 8. The figure portrayed that the OMKHES-MS model has resulted in superior SC values under every image. For instance, with Barbara image, the OMKHES-MS model has accomplished higher SC of 0.9986 whereas the whale optimization algorithm (WOA)-EBS and grey wolf optimizer (GWO)-EBS models have

attained lower SC of 0.9984 and 0.9984 respectively. Similarly, with Peppers image, the OMKHES-MS model has reached improved SC of 0.9987 whereas the WOA-EBS and GWO-EBS models have resulted in reduced SC of 0.9984 and 0.9985 respectively.

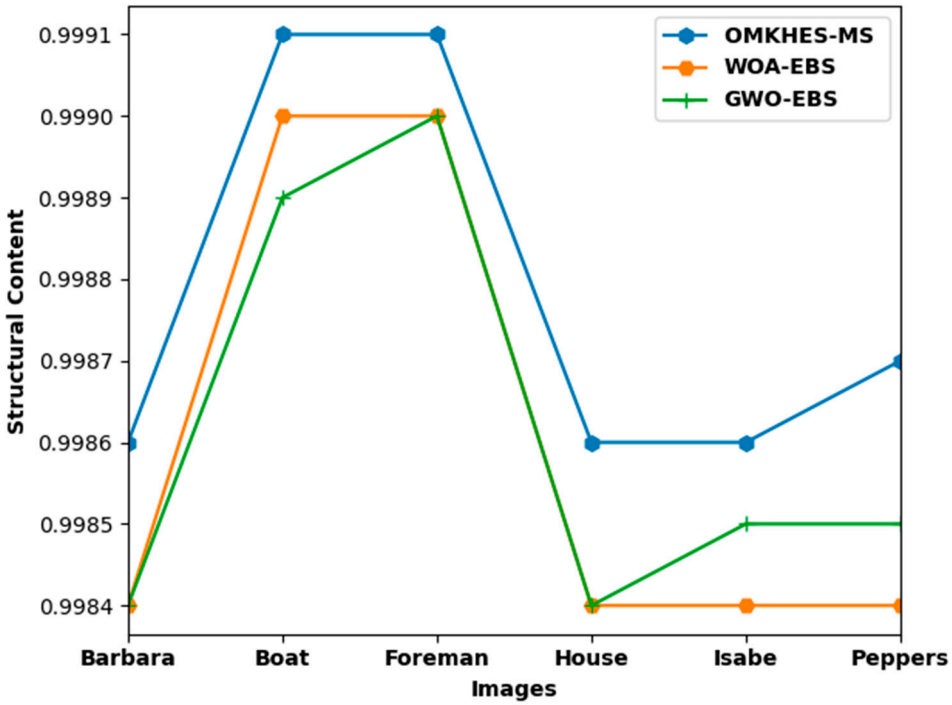

Figure 8. Comparative SC analysis of OMKHES-MS technique with existing models.

An extensive PSNR investigation of the OMKHES-MS model with recent approaches under distinct test images is made in Figure 9. The experimental values highlighted that the OMKHES-MS model has led to enhanced performance with increased PSNR values under every image. For instance, with Barbara image, the OMKHES-MS model has depicted superior PSNR of 59.4556 dB whereas the WOA-EBS and GWO-EBS models have exhibited inferior PSNR of 59.0647 dB and 53.4721 dB respectively. Likewise, with Peppers image, the OMKHES-MS model has exhibited increased PSNR of 62.3885 dB whereas the WOA-EBS and GWO-EBS models have implied decreased PSNR of 61.0412 dB and 58.4367 dB respectively.

A comprehensive AD and MD assessment of the OMKHES-MS model is compared with recent methods in Table 3. The experimental values notified that the OMKHES-MS model has gained effectual outcome with maximum values of AD and MD.

Table 3. AD and MD analysis of OMKHES-MS technique with different images.

Images	Average Difference			Maximum Difference		
	OMKHES-MS	WOA-EBS	GWO-EBS	OMKHES-MS	WOA-EBS	GWO-EBS
Barbara	0.0053	0.0066	0.0067	45.4132	47.2942	46.6040
Boat	0.0184	0.0194	0.0195	44.7870	46.8104	45.9838
Foreman	0.0282	0.0296	0.0296	53.5160	54.9844	54.8858
House	0.0009	0.0020	0.0022	53.1631	54.6097	54.3963
Isabe	0.0008	0.0018	0.0017	43.8986	46.3907	45.2574
Peppers	0.0005	0.0007	0.0008	47.0321	48.3379	49.8736

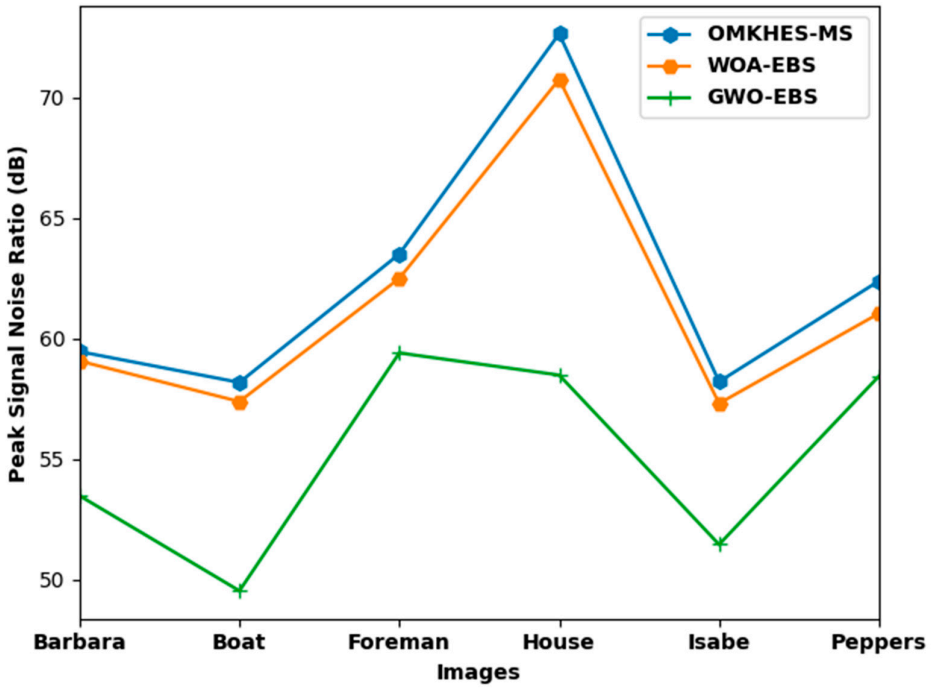

Figure 9. Comparative PSNR analysis of OMKHES-MS technique with existing models.

Figure 10 demonstrates the AD assessment of the OMKHES-MS model with existing models on dissimilar images. The results designated that the OMKHES-MS model has presented capable results with negligible values of AD over the other WOA-EBS and GWO-EBS models. For instance, with Barbara image, the OMKHES-MS model has gotten lesser AD of 0.0053 whereas the WOA-EBS and GWO-EBS models have presented greater AD of 0.0066 and 0.0067 respectively. Besides, with Pepper's image, the OMKHES-MS model has extended decreased AD of 0.0005 whereas the WOA-EBS and GWO-EBS models have delivered enlarged AD of 0.0007 and 0.008 respectively.

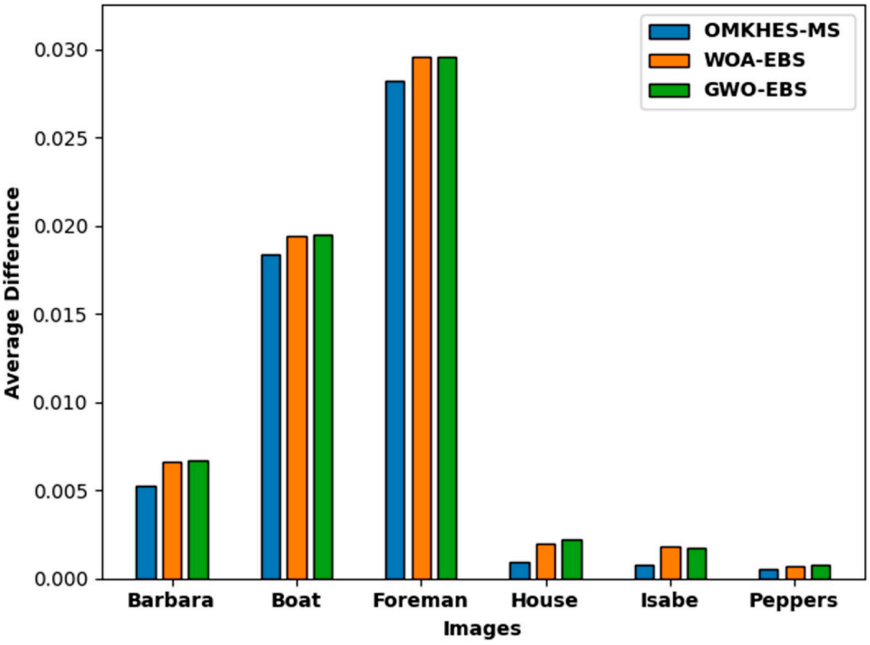

Figure 10. Comparative AD analysis of OMKHES-MS technique with existing models.

Figure 11 represents the MD inspection of the OMKHES-MS model with existing models on diverse images. The experimental values reported that the OMKHES-MS model has accomplished better performance with lower values of MD over the other WOA-EBS and GWO-EBS models. For instance, with Barbara image, the OMKHES-MS model has reached lessened MD of 45.4132 whereas the WOA-EBS and GWO-EBS models have realized increased MD of 47.2942 and 46.6040 respectively. In line with, Peppers image, the OMKHES-MS model has depicted insignificant MD of 47.0321 whereas the WOA-EBS and GWO-EBS models have revealed maximum MD of 48.3379 and 49.8736 respectively.

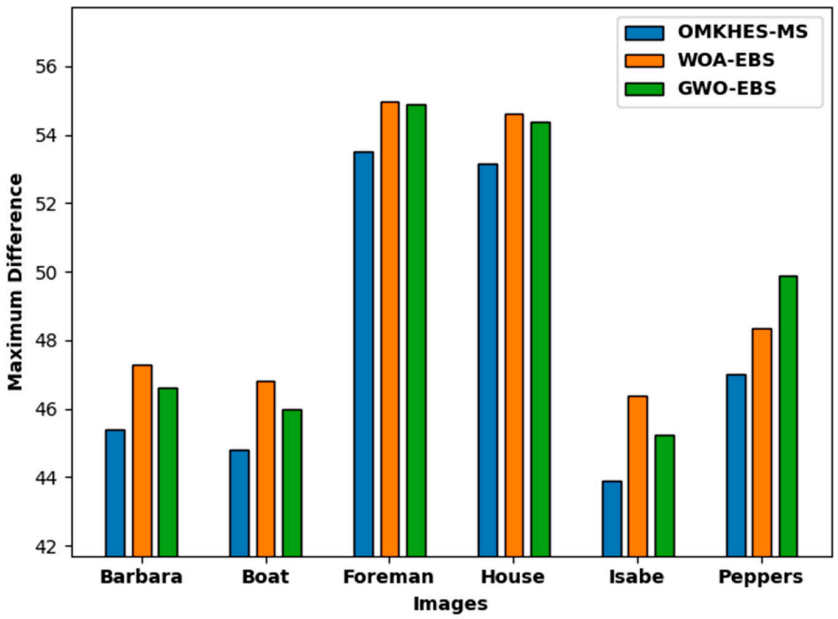

Figure 11. Comparative MD analysis of OMKHES-MS technique with existing models.

A comprehensive NCC and NAE assessment of the OMKHES-MS model is compared with recent methods in Table 4. The experimental values notified that the OMKHES-MS model has gained effectual outcome with maximum values of NCC and NAE. A broad NCC assessment of the OMKHES-MS model with compared methods under several test images is provided in Figure 12. The figure portrayed that the OMKHES-MS model has resulted in better outcomes with improved NCC values under every image.

Table 4. NCC and NAE analysis of OMKHES-MS technique with different images.

Images	Normalized Cross-Correlation			Normalized Absolute Error		
	OMKHES-MS	WOA-EBS	GWO-EBS	OMKHES-MS	WOA-EBS	GWO-EBS
Barbara	0.9985	0.9897	0.9905	0.0002	0.0016	0.0017
Boat	0.9980	0.9899	0.9899	0.0002	0.0010	0.0013
Foreman	0.9987	0.9910	0.9896	0.0001	0.0011	0.0013
House	0.9985	0.9906	0.9900	0.0010	0.0017	0.0023
Isabe	0.9994	0.9904	0.9907	0.0004	0.0014	0.0016
Peppers	0.9998	0.9918	0.9903	0.0008	0.0017	0.0020

For instance, with Barbara image, the OMKHES-MS model has reached superior NCC of 0.9985 whereas the WOA-EBS and GWO-EBS models have shown lesser NCC of 0.9897 and 0.9905 respectively. Equally, with Peppers image, the OMKHES-MS model has displayed increased NCC of 0.9998 whereas the WOA-EBS and GWO-EBS models have inferred diminished NCC of 0.9918 and 0.9903 correspondingly.

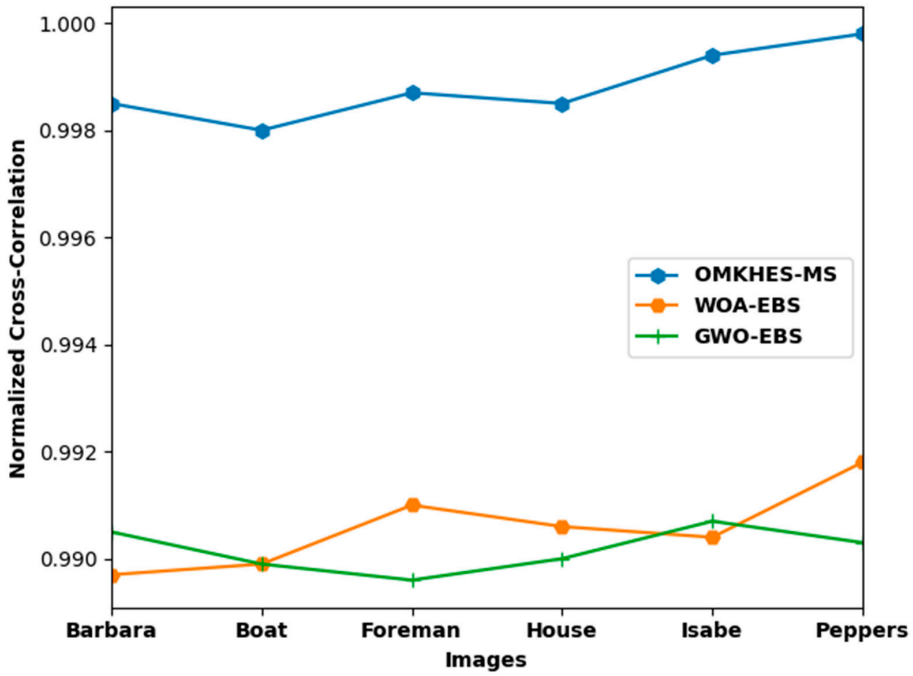

Figure 12. Comparative NCC analysis of OMKHES-MS technique with existing models.

Figure 13 illustrates the NAE analysis of the OMKHES-MS model with present models on diverse images. The simulation outcome revealed that the OMKHES-MS model has outperformed the other methods with least NAE values. For instance, with Barbara image, the OMKHES-MS model has reached decreased NAE of 0.0002 whereas the WOA-EBS and GWO-EBS models have realized increased NAE of 0.0016 and 0.0017 respectively. Moreover, with Peppers image, the OMKHES-MS model has portrayed negligible NAE of 0.0008 whereas the WOA-EBS and GWO-EBS techniques have presented supreme NAE of 0.0017 and 0.0020 respectively.

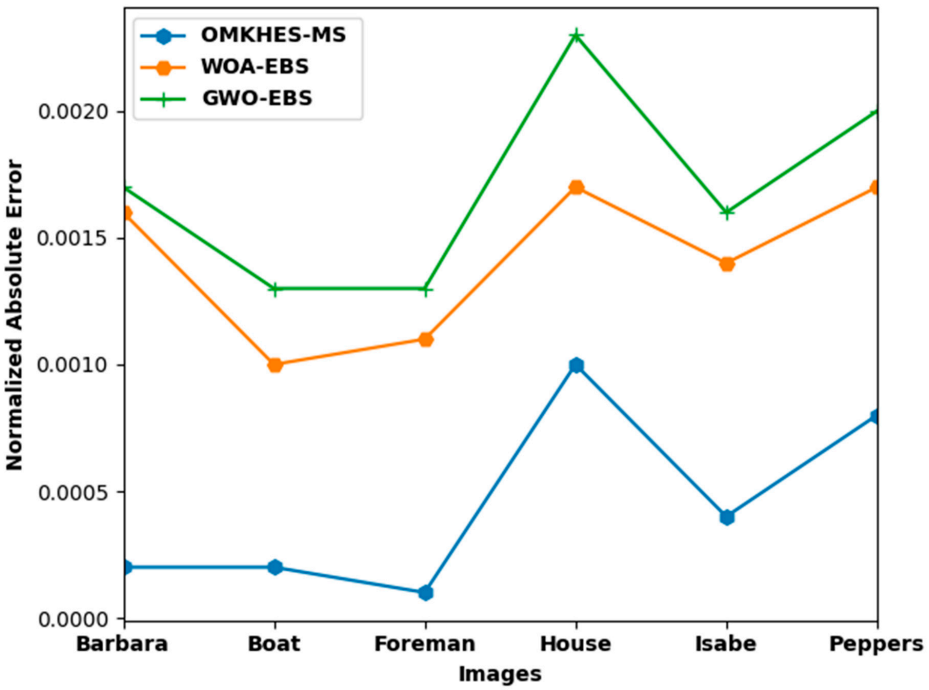

Figure 13. Comparative NAE analysis of OMKHES-MS technique with existing models.

From the detailed results and discussion, it can be clear that the OMKHES-MS model has reached superior results over the other methods interms of different measures. Therefore, the OMKHES-MS model can be utilized as an effective tool for accomplishing multimedia security in the IoE environment.

5. Conclusions

In this study, a new OMKHES-MS technique has been developed to accomplish security and privacy in the IoE environment. The OMKHES-MS model involves a series of processes namely SVD, COA based optimum pixel selection, MKHE based encryption, and PRO based key generation. Finally, the cipher image from the MKHE technique is embedded into the chosen pixel values of the cover image to generate stego image. The design of PRO algorithm helps in choosing optimum keys for the generation of cipher images. To investigate the enhanced performance of the OMKHES-MS model, a comprehensive simulation analysis is performed and the results are investigated under several aspects. The extensive comparative analysis reported the supremacy of the proposed model over the rennet approaches interms of different measures. Therefore, the OMKHES-MS model can be utilized as an effective tool to accomplish security in the IoE environment. In future, lightweight crytographic techniques can be designed for IoE environment. Besides, detailed security analysis of the OMKHES-MS model will be made in our future work.

Author Contributions: Conceptualization, I.A. and A.M.; methodology, H.A.M.; software, I.Y.; validation, S.S.A., M.M.A. and A.S.Z.; formal analysis, M.A.H.; investigation, I.A.; resources, M.A.H.; data curation, I.Y.; writing—original draft preparation, H.A.M.; writing—review and editing, A.M; visualization, A.M.; supervision, S.S.A.; project administration, M.A.H.; funding acquisition, H.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under grant number (RGP 2/45/43). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R114), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4210118DSR05). The authors would like to thank Prince Sultan University for its support in paying the Article Processing Charges.

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated during the current study.

Conflicts of Interest: The authors declare no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

References

1. Dudeja, R.K.; Bali, R.S.; Aujla, G.S. Internet of Everything: Background and Challenges. In *Software Defined Internet of Everything*; Springer: Cham, Switzerland, 2022; pp. 3–12.
2. Lu, H.; Su, S.; Tian, Z.; Zhu, C. A novel search engine for Internet of Everything based on dynamic prediction. *China Commun.* **2019**, *16*, 42–52.
3. Juneja, S.; Gahlan, M.; Dhiman, G.; Kautish, S. Futuristic cyber-twin architecture for 6G technology to support internet of everything. *Sci. Program.* **2021**, *2021*, 9101782. [CrossRef]
4. Petrescu, M.; Krishen, A.; Bui, M. The internet of everything: Implications of marketing analytics from a consumer policy perspective. *J. Consum. Mark.* **2020**, *37*, 675–686. [CrossRef]
5. Sajid, M.; Harris, A.; Habib, S. Internet of Everything: Applications, and Security Challenges. In Proceedings of the 2021 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 9–10 November 2021; pp. 1–9.
6. Padhi, P.; Charrua-Santos, F. 6G Enabled Industrial Internet of Everything: Towards a Theoretical Framework. *Appl. Syst. Innov.* **2021**, *4*, 11. [CrossRef]
7. Wang, M.; Zhou, Z.; Ding, C. Blockchain-Based Decentralized Reputation Management System for Internet of Everything in 6G-Enabled Cybertwin Architecture. *J. New Media* **2021**, *3*, 137–150. [CrossRef]
8. Sadi, M. Homomorphic encryption. In *Emerging Topics in Hardware Security*; Springer: Cham, Switzerland, 2021; pp. 281–307.
9. Zhang, Z.; Cao, S.; Yang, X.; Liu, X.; Han, L. An efficient outsourcing attribute-based encryption scheme in 5G mobile network environments. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3488–3501. [CrossRef]

10. Srivastava, V.; Debnath, S.K.; Stănică, P.; Pal, S.K. A multivariate identity-based broadcast encryption with applications to the internet of things. *Adv. Math. Commun.* **2021**. [CrossRef]
11. Pant, S.; Sharma, M.; Sharma, D.K.; Gupta, D.; Rodrigues, J.J.P.C. Enforcing Intelligent Learning-Based Security in the Internet of Everything. *IEEE Internet Things J.* **2021**, *1*. [CrossRef]
12. Karthiban, M.K.; Raj, J.S. Big data analytics for developing secure internet of everything. *J. ISMAC* **2019**, *1*, 129–136.
13. Mohanty, S.P.; Yanambaka, V.P.; Kougianos, E.; Puthal, D. PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE). *IEEE Consum. Electron. Mag.* **2020**, *9*, 8–16. [CrossRef]
14. Miao, Y.; Liu, X.; Choo, K.-K.R.; Deng, R.H.; Wu, H.; Li, H. Fair and Dynamic Data Sharing Framework in Cloud-Assisted Internet of Everything. *IEEE Internet Things J.* **2019**, *6*, 7201–7212. [CrossRef]
15. Singh, P.; Nayyar, A.; Kaur, A.; Ghosh, U. Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities. *Futur. Internet* **2020**, *12*, 61. [CrossRef]
16. Li, Z.; Tian, Y.; Zhang, W.; Liao, Q.; Liu, Y.; Du, X.; Guizani, M. RR-LADP: A Privacy-Enhanced Federated Learning Scheme for Internet of Everything. *IEEE Consum. Electron. Mag.* **2021**, *10*, 93–101. [CrossRef]
17. Mohammed Abdelkader, E.; Moselhi, O.; Marzouk, M.; Zayed, T. HybridElman neural network and an invasive weed optimization method for bridge defect recognition. *Transp. Res. Rec.* **2021**, *2675*, 167–199. [CrossRef]
18. Rezk, H.; Fathy, A.; Aly, M. A robust photovoltaic array reconfiguration strategy based on coyote optimization algorithm for enhancing the extracted power under partial shadow condition. *Energy Rep.* **2021**, *7*, 109–124. [CrossRef]
19. Chen, H.; Dai, W.; Kim, M.; Song, Y. Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference. In In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 395–412.
20. Moosavi, S.H.S.; Bardsiri, V.K. Poor and rich optimization algorithm: A new human-based and multi populations algorithm. *Eng. Appl. Artif. Intell.* **2019**, *86*, 165–181. [CrossRef]