Multimedia Tools and Applications (2023) 82:21005–21018
https://doi.org/10.1007/s11042-023-14526-7

An optimal and efficient data security technique through crypto-stegano for E-commerce

Dulal Kumbhakar[1] · Kanchan Sanyal[2] · Sunil Karforma[3]

Received: 5 August 2021 / Revised: 26 April 2022 / Accepted: 31 January 2023 /
Published online: 8 February 2023

Abstract

E-Commerce or Electronic commerce is the buying and selling of goods and services in which any commercial transactions through wireless electronic devices such as hand-held computers (tablets), mobile phones or laptops is conducted anytime & anywhere via Internet technology. But, E-Commerce transactions or services are suffered by many attacks such as Man in the Middle attack, eavesdropping attacks, and etc. due to the lack of secured security infrastructure. Here, data security is one of the ways to keep the confidential information secure through E-Commerce transactions. In this connection, we have proposed an optimal and efficient data security with the combination of Elgamal cryptosystem and LSB image steganography technique for E-Commerce. In our proposed work, at the merchant side, Elgamal encryption technique is used to protect sensitive information during E-Commerce transactions from intruders and LSB image steganography process is also applied to hide generated Elgamal encrypted data and produce a stego-image (steganography image). Then, DCT (Discrete Cosine Transform) technique through autoencoder is imposed on stego-image to make an optimal image to increase the throughput of the work. After that, the produced optimal image with cipher text is sent to the customer end. At the customer end, first, stego-image is extracted from the optimal image using LSB retrieval process. Then, Elgamal decryption process is used to retrieve the original data and secure the E-Commerce transactions in efficiently. Based on the experiment, we have plotted the performance metrics such as MSE, PSNR and SSIM on the work and entropy of the optimal image is also calculated with respect to the sample image. Thereby, a high level performance metrics is obtained in our proposed work.

Keywords E-commerce · Elgamal cryptosystem · LSB steganography · DCT with autoencoder · Performance metrics

✉ Dulal Kumbhakar
dulalkumbhakar69@gmail.com

[1] Department of B.C.A., Vivekananda Mahavidyalaya, Hooghly, West Bengal, India

[2] Department of Computer Application, Bhadrapur M.N.K High School, Birbhum, West Bengal, India

[3] Department of Computer Science, The University of Burdwan, Bardhaman, West Bengal, India

1 Introduction

E-Commerce is already entering possible in all areas of business, customer care services, new product development and design. Hence, E-Commerce acts as a new business model that exchanges the valuable services (buying and selling goods) among the business organizations and the end customers based on the Wireless Application Protocol (WAP). Hence, the integration of Internet, Wireless and E-Commerce produces a successful E-Commerce [1].

The implementation of social distancing, lockdowns and other respective parameters during COVID-19 pandemic situation has led customers to escalate online E-Commerce services such as online shopping, electronic payments, online auctions, Internet Banking, social media use, online conferencing, and streaming of videos and films. In this regard, in 2020, retail E-Commerce sales worldwide amounted to 4.28 trillion US dollars and e-retail revenues are projected to grow to 5.4 trillion US dollars in 2022 [14].

Data security management in E-commerce E-Commerce data security is a set of protocols that ensures secure transactions over the internet. There are several kinds of security attacks such as Man in the Middle attack, eavesdropping attacks and brute force attacks may arise on the E-Commerce transactions. So, we need to give more attention on the data security. The common security requirements are authentication of merchant and customer, confidentiality of data, integrity of data and non-repudiation. The overall aim of these security requirements is to protect the credential information of the customers as well as organizations. E-Commerce data security process has several major steps [19] which are (a) Identify the security threats and risks (b) Build a security policy (c) Prepare an implementation plan (d) Review for access and evaluation of security procedures and increase the security awareness. In this work we have focused on implementation plan to mitigate the security threats in E-Commerce transactions.

Cryptography in E-commerce Since, security attacks are being associated in E-Commerce, the use of cryptography provides highly secure and efficient framework for E-Commerce transactions, so that it uses different encryption and decryption techniques. Here, encryption process is the conversion of plaintext into cipher text so that intruders cannot read it and decryption is the reverse process of encryption for transforming the cipher text into plaintext. The cryptographic mechanisms are basically two types such as private or symmetric cryptography and public or asymmetric cryptography regarding key generation [20]. Regarding to the importance of E-Commerce, if there is no secure encryption technique, then there is a high possibility of data breach and personal credentials can be easily manipulated by intruders. Hence, with the help of public or private key cryptographic techniques such as RSA, ECC, EC- Elgamal and AES, the data can be easily encrypted to achieve effective security on the E-Commerce environment.

In this context, Elgamal encryption public key cryptographic algorithm is used in the proposed work for key generation, encryption and decryption of secret data. It was first proposed by Taher Elgamal in 1985 is based on Deffie Hellman Key Exchange (DHKE). Its security lies on the intractability of the Discrete Logarithm Problem and Deffie Hellman Problem [13].

Steganography with optimal technique in E-commerce Steganography, comes from Greek words STEGANOS and GRAPHIE, which means “covered and writing” [21] is a technique of

hiding information by concealing the secret message into a digital image, video or audio and text file. Steganography is applicable for storing secret data, confidential data communication and protection of data modification in E-Commerce [17]. Again, optimal technique is generally used to reduce the time as well as space complexity of the work [11]. In our proposed work, LSB image steganography is used to hide the information and also then DCT (Discrete Cosine Transform) is used to achieve optimal image form through high embedded efficiency. In addition, simple autoencoder is applied on optimal image for learning a compressed representation of original data.

The paper is organized as follows. Section 2 represents related works regarding information security framework. Section 3 focuses the contribution of our proposed work and section 4 proposes optimal and efficient data security framework through Elgamal cryptosystem and Steganography mechanism. Section 5 depicts the experimental evaluation and performance metrics of the proposed work with comparative analysis. Section 6 concludes the paper.

2 Related works

During the past few years, many researchers have been contributed their works in the field of information as well as data security perspective.

Eshraq S. Bin Hureib and Adnan A. Gutub [5] have implemented a technique through combining two methods, namely, Elliptic curve cryptography and image steganography in which secret information is encrypted and then it is hided so as to increase the security level in medical data as well as business related information. Here, information text is encrypted using Elliptic Curve Cryptography in the first stage. After that image steganography i.e. LSB technique is used in the second stage to conceal the information text from the attackers. For performance evaluation, Peak Signal to Noise Ratio (PSNR) is applied on the stego-images and then performance comparison between ECC and RSA algorithms have been done.

R.Ganesh Prabu and Dr.K.Latha [11] have proposed a hybrid crypto stegano system that assembles the crypto and stegano techniques. This work provides the high level security over the secret information transmission through asymmetric based Elgamal cryptography. It also hides the information through steganographic process using quantum LSB image steganography and also with the help of eagle strategy particle swarm optimization algorithm; a cover image is optimized so that the large amount of information can be transferred through the wireless connection in securely.

K. Muhammad et al. have proposed a secure framework of image steganographic through using stego key-directed adaptive least significant bit (SKA-LSB) substitution method and multi-level cryptography for secure communication over the public network. In this work, a two-level encryption algorithm (TLEA) is used to encrypt the stego-image and secret data is also encrypted by a multi-level encryption algorithm (MLEA). After that the encrypted information is then embedded with the host image based on an adaptive LSB substitution method. They evaluated the performance of the proposed framework quantitatively and qualitatively through various image quality assessment measurements such as peak-signal-to-noise-ratio (PSNR), structural-similarity-index metric (SSIM), and root-mean-square-error (RMSE) for making better stego-image quality. Finally, they have concluded that the proposed framework is computationally reasonable and highly secure compared to other related techniques [10].

D. kumbhakar et al. proposed a secure and efficient end-to-end authentication technique using ECDSA algorithm in E-Commerce transactions. Here, ECDSA algorithm uses scalar random in point multiplication k*n (k is the random number) so that strong randomness in ECDSA algorithm increases the authentication security level of E-Commerce transactions. They have also plotted the summary performances of ECDSA compared to RSA and DSA algorithms respectively and showed that ECDSA with same level of security offers faster implementations by consuming less memory relatively compared to existing works [8].

Marwa E. Saleh et al. proposed a hybrid technique with the combination of cryptography and steganography mechanisms to improve the data security. In this work, firstly, the Advanced Encryption Standard (AES) algorithm has been revised and used to gain high level security through modified AES_MPK encryption algorithm. Secondly, the encrypted data has been hidden by PVD-MSLDIP-MPK image steganography technique. Therefore, two layers of security protection are achieved using the proposed technique in the work. Further, the performance of the proposed technique is evaluated by stego-image quality measurement parameter i.e. PSNR. Hence, the proposed technique with PSNR parameter performance provides high embedding capacity and high quality stego images [15].

3 Our contributions

Although many researchers worked on the E-Commerce data security to secure data transmission, but many security threats like Man in the Middle attack and eavesdropping attacks are still active regarding any E-Commerce transactions or services. In other words, many security mechanisms have been developed in respect of E-Commerce services or transactions, but these existing works may not be sufficient in overcoming the said security threats. In [11] a hybrid crypto stegano mechanism is proposed through optimization technique but the procedure of the proposed optimization technique is not efficient. In [8] a secure and efficient end-to-end authentication system is developed with the combination of two known cryptography algorithms only. Again, this work is mainly focused on the time complexity only, so that this work is not sufficient to overcome the security breaches during E-Commerce transactions. Further, [15] proposed a merged technique through cryptography and steganography mechanisms to improve the data security. In this work, PSNR metric is used to measure the stego-image quality but the proposed technique gives comparatively lower PSNR. Therefore, this work is not appropriate to achieve optimum level data security.

Regarding E-Commerce security issues, we have introduced an optimal and efficient data security system for E-Commerce. The novelty of our proposed work is that, firstly, Elgamal protocol is used to protect the sensitive information from the attackers during E-Commerce transactions. In addition, LSB image steganography is applied as second layer protection to hide the generated cipher text by Elgamal encryption technique and also stego-image is produced. After that, optimization of the stego-image i.e. optimal image is done through DCT mechanism with autoencoder to achieve high embedded efficiency in the proposed work. The main objective of the work is to enhance the security level as well as performance efficiency as compared with existing techniques regarding E-Commerce security aspects.

4 Proposed work

Our proposed system is classified into five phases as Elgamal encryption, LSB image steganography, optimal image with DCT, Image extraction, Elgamal decryption and verification. The optimal based data security framework of proposed work is shown in the following Fig. 1.

The following steps are involved in the proposed framework.

1. The customer selects the item(s) to be purchased and provides the details to the merchant.
2. Merchant calculates the key pair (P_{V1}, P_{B1}) using Elgamal encryption technique.
3. Merchant encrypts the plain text into cipher text using his private key (P_{V1}).
4. Then, hides the cipher text using LSB steganography method to generate a stego-image.
5. Also, the stego-image is turned into optimal image using DCT with autoencoder in the merchant side.
6. After that, transfer the optimal image with Elgamal public key (P_{B1}) to the customer end.
7. At the customer end, customer extracts the cipher text from the optimal image using LSB reveal method.
8. Then, decrypts the cipher text using his private key (P_{V2}) to generate the plaintext and then this generated plaintext data is compared with original transmitted data from the merchant side.

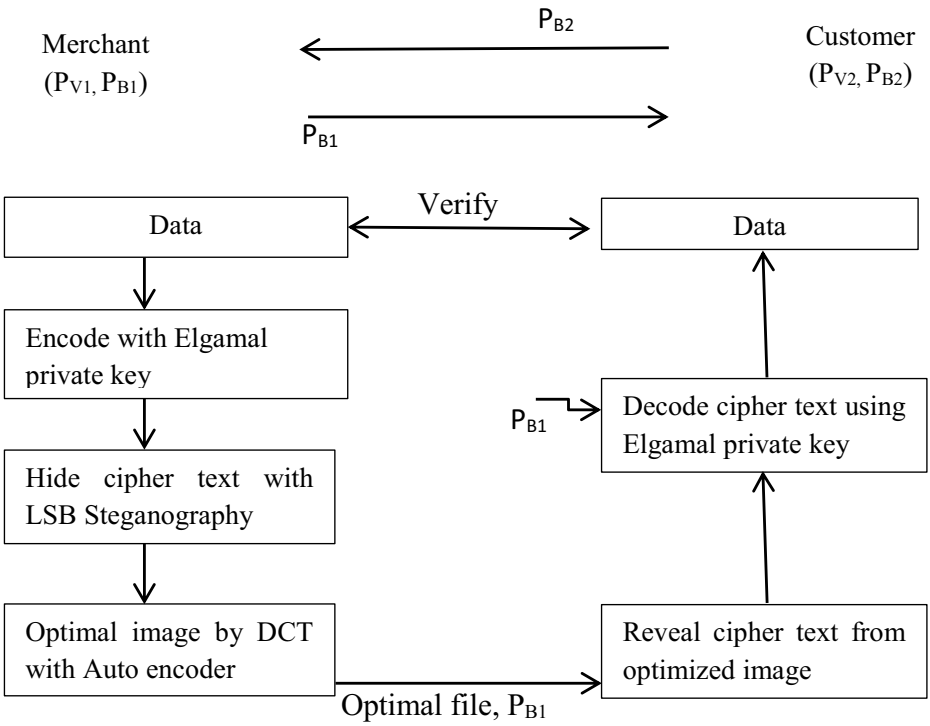

Fig. 1 Optimal based data security framework

9. Finally, if the verification is successfully done that is the generated data on the customer side is same as the merchant's transmitted data is same, then the transaction or communication between merchant & customer will be proceed. Otherwise it will be rejected.

A. Elgamal Encryption phase

This phase is the initial phase of the proposed framework and it gives the confidence that the merchants' data or message cannot be decrypted by anyone other than the authorized recipient. It consists of two parts as (i) Key generation and (ii) Encryption process. The following steps regarding key generation and encryption are explained below [4]:

i. Key generation:

Step-1: A very large prime number p is chosen and then α is chosen as primitive root modulo p.
Step-2: Compute $\beta = \alpha^a \pmod p$, where 'a' is the chosen random integer in the range of $1 < a < p-1$.
Step-3: The encryption key (p, α, β) is made as public and 'a' acts as a private key.

ii. Encryption:

Step-1: Merchant selects a secret integer 'b' and calculates $r \equiv \alpha^b \pmod p$ and $t \equiv \beta^b.m \pmod p$, where 'm' is the initial message to be submitted.
Step-2: Finally, merchant's encrypted message $c = (r, t)$ and integer 'b' is the merchant's private key (P_{V1}).

Our proposed Elgamal encryption cryptosystem is based on the Discrete Logarithm problem so that the transferred information is not exposed by intruders using a randomized encryption exponent regarding E-Commerce transactions between merchant and customer end.

B. LSB image steganography phase

After Elgamal encryption, LSB image steganography technique is proposed for hiding or masking the secret information inside the image to secure communication between merchant and customer end. In our work, generated encrypted data in the previous phase is hidden by LSB image steganography. This LSB approach is used to embed the data bits into the least significant bits of cover image in the merchant side (Figs. 2, 3, 4).

The following steps of LSB image steganography are as follows [17]:

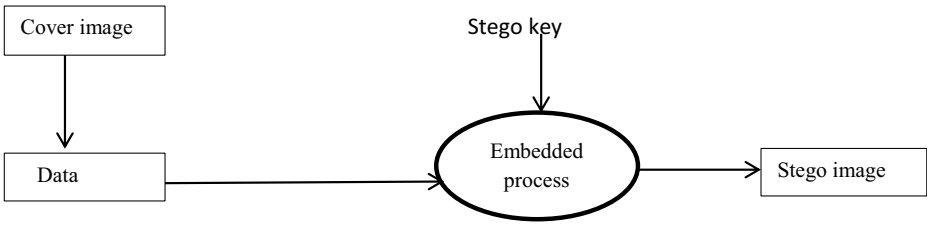

Fig. 2 LSB image steganography block diagram

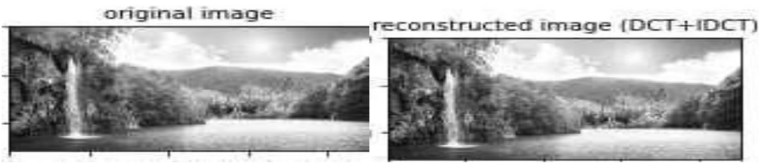

Fig. 3 Optimal image by DCT

Step 1: Merchant selects any cover image in which the data is to be hidden.
Step 2: Then, converts the generated Elgamal encrypted data into binary.
Step 3: Also, Determines LSB of each pixels of the selected cover image.
Step 4: After that merchant replaces LSB of the selected cover image with every bit of encrypted data one by one.
Step 5: Continue this replacement process until all bits are to be embedded for generating a stego-image.

C. Optimal image phase

Optimal technique helps us to increase the throughput as well as embedded efficiency of the proposed system. In this phase, the discrete cosine transform (DCT) tool is used for image compression. DCT is a mathematical tool that is used to get optimization of generated stego image in the system. The following steps are involved in our proposed optimal phase using DCT on the merchant side [6, 9].

Step-1: Firstly, generated stego-image in the previous phase is divided into 8 × 8 blocks.
Step-2: Then, each block is modified to work on pixel values ranging from −128 to 127 designed by DCT.
Step-3: The modified block is multiplied by designed DCT matrix to apply DCT in each block.
Step-4: After that, each block is compressed through Quantization and it is also then entropy encoded.

Generated optimal image is look like below:

For training the optimal image, simple autoencoder is applied using keras library to visualize the optimize error and loss of the optimal image. Here, optimize error indicates the fault while reconstructing the optimal image and loss function specifies the difference between the actual optimal image and reconstructed image [2]. Look like as below:

This generated optimal image with Elgamal public key (P_{B1}) is sent to the customer end.

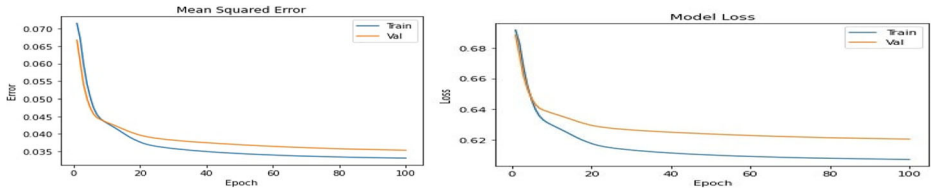

Fig. 4 Optimize error and loss of the model

D. Image extraction phase

In this phase, customer extracts stego-image from the optimal image using LSB reveal method. The following steps are involved for retrieving cipher text from optimal image [3].

Step-1: Firstly, customer read the stego-image.
Step-2: Then, finds the length of the secret message from the first pixels.
Step-3: Customer also calculates LSB of each pixel of the stego-image.
Step-4: Then, bits are retrieved and convert each 8 bit into characters.
Step-5: Continue this retrieval process until the cipher text.is retrieved.

E. Elgamal decryption and verification phase

In this phase, customer decrypts the cipher text into the plaintext using Elgamal decryption process. Since, Elgamal cryptosystem is the asymmetric public key mechanism, so that there are different keys at merchant as well as customer used for secure data security in E-Commerce. Hence, only public key is sharable, but private keys are not and the decryption is done by customer using his private key. The steps against decryption & verification are listed below:

Suppose, (p, α, β) is the public key (P_{B2}) and 'a' is a private key (P_{V2}) of the customer end.

Step-1: Customer can compute the message 'm' $= t.r^{a} \pmod p$, where (r, t) is the cipher text and 'a' is the merchant's private key (P_{V2}).
Step-2: Then, finds original plaintext (m) which is send by the merchant.
Step-3: Finally, transmitted data is verified with decrypted data that is if $m \equiv t.r^{a} \equiv t.\beta^{-k} \pmod p$, then the communication between merchant and customer is successfully done.

In this context, if intruders want to crack Elgamal encryption key (p, α, β) that means they want to recover the secret integer 'a' such that $\alpha^{a} = \beta \pmod p$. Its solution would be obtained using a discrete logarithm and if one computes $\log_{\alpha}\beta$, but it gives roughly floating point number, not an integer at all. So that presumably a computation for obtaining a key is too difficult practically.

Therefore, Elgamal cryptosystem provides a secure and effective security infrastructure to protect the data from the attacks such as Man in the Middle attack and eavesdropping attacks as compared with existing cryptography techniques in respect of E-Commerce transactions between merchant and customer.

5 Experiments

Jupiter notebook IDE and python 3.8 are used for the execution of our proposed system. Further, keras library, pycrypto and opencv packages are used for autoencoder implementation, cryptographic algorithms and image processing respectively. Now, we elaborate the several metrics which are applied in the proposed system to visualize the system performance.

5.1 Work performance with parameter metrics

Here, MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio) and SSIM (Structural Similarity Index) are used to compare the performance of the proposed work with the existing techniques. For comparison, bar charts have been drawn in respect of performance metrics.

A. MSE

MSE is the squared error between the decompressed and the original image [7]. It is used to get excellence quality of the generated optimal stego-image in the proposed work.

$$\mathbf{MSE} = \frac{\sum_{I,J} [\mathbf{X1}(\mathbf{A},\mathbf{B}) - \mathbf{X2}(\mathbf{A},\mathbf{B})]^2}{\boldsymbol{I}*\boldsymbol{J}} \tag{1}$$

Where X1(A, B), X2(A, B) are origin image and generated optimal stego-image respectively and I x J represents the number of rows and columns in the images (Fig. 5).

B. PSNR

The quality assessment of the generated optimal stego-image is measured by PSNR. It computes the peak signal-to-noise ratio, in decibels, between the original image and generated optimal image. Here, high PSNR gives the better the quality of the optimal image.
So, PSNR is calculated in decibels as:

$$\begin{aligned} \text{PSNR} &= 10\log10\left(\frac{MX_1^2}{MSE}\right) = 20\log10\left(\frac{MX_1}{\sqrt{MSE}}\right) \\ &= 20\log10\,(MX_1) - 10\log10\,(MSE) \end{aligned} \tag{2}$$

Where, MX_1 is the maximum possible pixel value in the input image. When the pixel is represented using 8 bit unsigned integer data type per sample, MX_1 is 255 [12].

C. SSIM

SSIM is a perceptual based metric that measures the image degradation which is caused by image compression or by losses through data transmission. It requires two images for quantifying the similarity from the same image capture process [16]. In our proposed system, SSIM specifies the normalized mean value regarding quality performance of optimal stego-image based on original cover image.

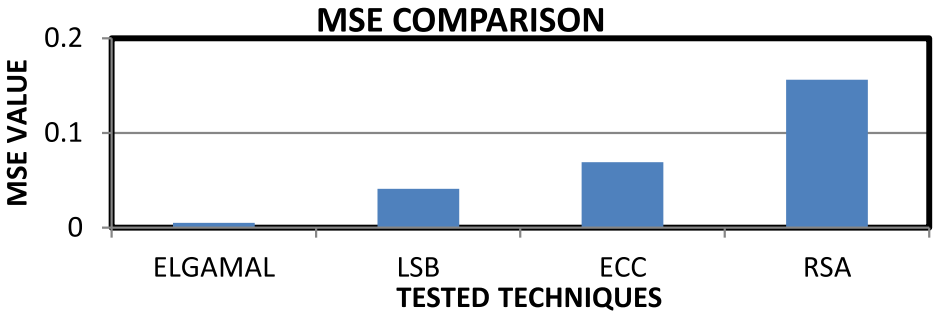

Fig. 5 MSE Comparison

Performance parameter metrics are plotted with respect to existing techniques such as LSB, ECC and RSA in the Figs. 6, 7, 8 respectively. Hence, the MSE of proposed Elgamal methodology is relatively small as compared to existing methodology (0.0059, 0.0410, 0.0690, and 0.1567). The proposed methodology gives good PSNR as compared to existing techniques (75.17, 66.76, 64.51 and 60.94). Further, the proposed methodology provides high efficiency performance regarding structural index of the optimal image as compared to existing techniques (0.9999, 0.9998, 0.9998, and 0.9997). Thus, the proposed Elgamal methodology regarding E-Commerce data security provides good performance metrics as compared to existing techniques.

Further, in this work, we have taken five sample images, namely, Earth, Trees, Ocean, Turtle and Tiger, to encode and measure the performance parameter metrics (Tables 1 and 2).

We have also plotted the corresponding histogram graphs of optimal images by intensity levels and respective pixel values. In this work, histogram is used to specify the distribution of luminance or color of the optimal images (Fig. 9).

5.2 Work performance with entropy

Here, entropy is applied to measure the randomness of the image. Thus, entropy is used as criteria assessment for the significance of ciphering technique in the proposed work. The entropy is defined as follows [18]:

$-\sum_{i=0}^{n-1} P_i \log_a P_i$, where 'n' is the number of gray levels, P_i is the probability of a pixel, and 'a' is the base of the logarithm function.

The entropy of the chosen sample images and their corresponding optimal images is plotted in the Table 2.

5.3 Comparative analysis

Our proposed hybrid approach that combines two techniques, namely, Elgamal encryption and LSB image steganography is contributed in the field of E-Commerce data security regarding any transactions between merchant and customer. In our proposed work, at the first stage, the Elgamal encryption technique is used to encrypt the data in securing the security requirements such as data confidentiality, customer authenticity and privacy of E-Commerce transactions as they are communicated via insecure public network. Regarding performance of Elgamal

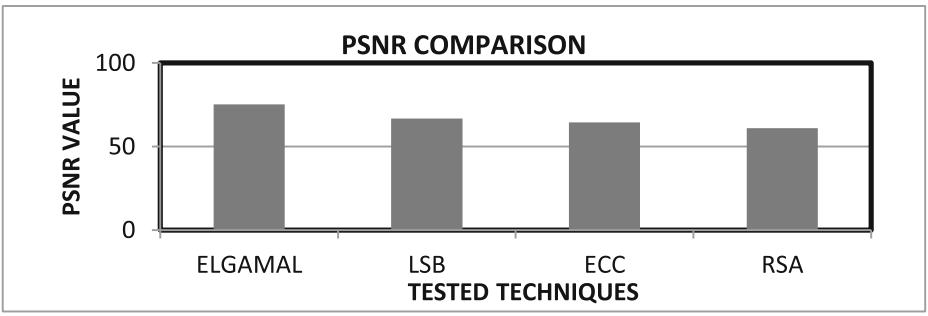

Fig. 6 PSNR Comparison

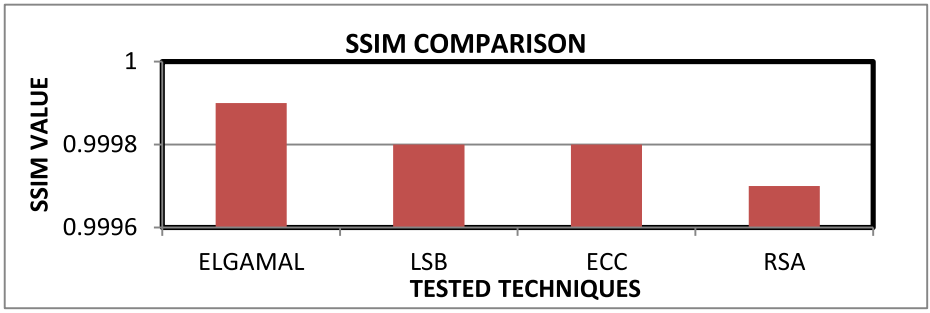

Fig. 7 SSIM Comparison

encryption with existing techniques, we have already plotted the performance metrics PSNR, MSE and SSIM in the Figs. 5, 6, 7 respectively. From the figures, we have observed that our proposed Elgamal encryption technique provides higher PSNR, lower MSE and higher structural index values compared to existing tested techniques such as RSA, ECC and LSB and hence, this proposed technique helps to increase the security level regarding E-Commerce transactions. Again, at the second stage, LSB image steganography is used as additional security protection to hide the encrypted cipher text by randomly chosen images and encode to produce a stego-image so that a high level security infrastructure regarding E-Commerce transactions or services against any security breaches can be achieved. After that DCT image compression tool with simple autoencoder is imposed on the stego-image to make an optimal image and as a result of that a high embedded efficiency based on the security performance can be obtained in the proposed work. Here, simple autoencoder indicates the optimize error and loss of the optimal image.

In this context, if we compare our proposed optimal work with the existing work [15] then it can be say that they [15] have, firstly, used the modified Advanced Encryption Standard (AES) algorithm to encrypt the secret data and then the encrypted message is hidden by image steganography technique to achieve two layer security protections of the secret data. But, there is no any suitable image compression technique used so that the optimum level security performance can be obtained. Therefore, existing work [15] obviously gives comparatively lower PSNR values of the stego-images than our optimal work and hence, [15] work may not be appropriate to improve the embedded efficiency regarding security performance.

Again, in the existing work [11], an optimized crypto stegano system has also been introduced for the data security of defense applications but the procedure of the work

Sample encoded images

Corresponding optimal images

Fig. 8 Sample encoded images with their optimal forms

Table 1 Performance metrics of respective optimal images

Sl.No	Sample image	MSE	PSNR	SSIM
1	Earth	0.0068	74.57707	0.999963
2	Trees	0.0076	74.07141	0.999997
3	Ocean	0.0059	75.17021	0.999982
4	Turtle	0.0127	71.85477	0.999965
5	Tiger	0.0065	74.76593	0.999996

framework is different from our optimal work in respect of optimization. They [11] have, firstly, used Elgamal encryption technique to encrypt the secret information and then selected cover images have been optimized through Eagle Strategy Particle Swarm Optimization. After that Quantum image steganography technique is applied to make a stego-image and this produced stego-image is then transferred to the receiver end. In this context, our selected optimization technique (DCT) is applied after the creation of a stego-image in achieving a fully optimal image form to improve the work performance efficiency and this optimal form is then communicated via insecure channel instead of stego-image. Hence, it can be concluded that the work [11] could not reach at the maximum level of optimization regarding security performance. Nevertheless, the proposed optimal technique has better embedded efficiency and approximate same performance parameter metric PSNR as compared to existing work [11]. Although, the chosen cover images are resized as 2000 × 2000 pixels in the existing work [11] whereas 144 × 144 pixels resized images are used in the proposed optimal work to compute the performance parameter metrics in the work. Thereby, our proposed work based on the performance efficiency is highly optimized and secured as relatively compared to other existing works.

Further, we have computed the entropy of the chosen sample images and their corresponding optimal images to measure the randomness of the image information. This is shown in the Table-2 and it is clearly observed that the entropy of the corresponding optimal images is to have as close entropy to the entropy of the original sample images and hence, our applied Elgamal encryption technique as well as LSB image steganography technique is entropically secure as it is computationally infeasible for attackers to retrieve any information about the E-Commerce data from the corresponding optimal images. Therefore, our proposed hybrid approach based on the performance metrics with entropy measurement is more safe and robust compared to other existing techniques.

6 Conclusion

Nowadays, we depend on the internet for everything and hence the use of E-Commerce services and applications are increased very fast everywhere. In this regard, a secure

Table 2 Entropy of sample images with corresponding optimal images

Sample image Entropy	Trees	Ocean	Tiger	Earth	Turtles
Entropy of sample images	7.725	7.794	7.693	6.688	7.759
Entropy of corresponding optimal images	7.725	7.794	7.693	6.690	7.759

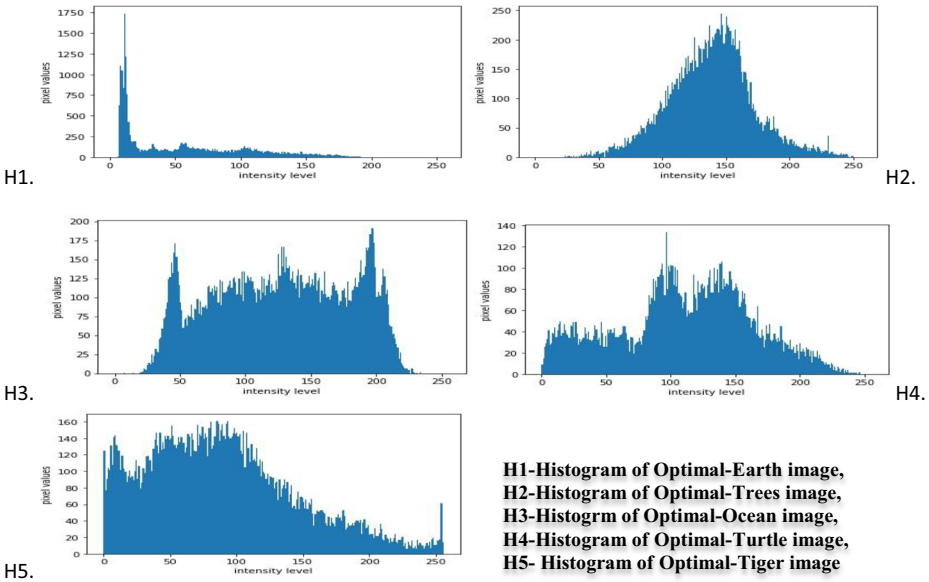

Fig. 9 Histogram graphs of Optimal-images

framework for transferring sensitive information through network is required to protect. Hence, we have proposed an optimal and efficient data security mechanism for E-Commerce transactions services. In this proposed work, we have implemented the two layers optimal based security framework that combines the Elgamal cryptosystem and LSB steganography for secure and effective E-Commerce transactions between merchant and customer. Here, asymmetric key based Elgamal cryptography is used to overcome the security related issues such as Man in the Middle attack and eavesdropping attacks, etc. In addition, LSB steganography is also used in the proposed work to hide the information with cover image to gain additional security and efficient implementation. Then, optimization is done by DCT tool to increase the embedded efficiency of the work and for that optimize error and loss of the optimal image are visualized using autoencoder. However, the aim of our proposed work is to provide the high level security infrastructure regarding E-Commerce transactions. Further, we have analyzed the performance of proposed work by various performance metrics such as MSE, PSNR and SSIM and compared with existing techniques. Finally, entropy of the optimal image as well as sample image is also calculated so that a better and enhancement security performance of our proposed system can be achieved.

Declarations

Conflict of interest There is no conflict of interest.

References

1. Deepika A (2018) Trends in M-commerce. Shanlax Int J Commerce 6(S1):285–290. https://doi.org/10.5281/zenodo.1419466
2. Dumas T, Aline R, Guillemot C (2018) Autoencoder based image compression: Can the learning be quantization independent?. arXiv:1802.09371v1

3. El_ Rahman SA (2015) A comprehensive image steganography tool using LSB scheme. Int J Image, Graphics Signal Process (IJIGSP) 6:10–18. https://doi.org/10.5815/ijigsp.2015.06.02
4. Elgamal T (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31(4)
5. Hureib ESB, Gutub AA (2020) Enhancing medical data security via combining elliptic curve cryptography and image steganography. IJCSNS Int J Comput Sci Netw Secur 20(8):1–8
6. Kumar V, Kumar A, Bhardwaj A (2012) Performance evaluation of image compression techniques. IEEE 2012 International Conference on Devices, Circuits and Systems (ICDCS 2012), (0), 447–450. https://doi.org/10.1109/icdcsyst.2012.6188797
7. Kumar R, Sharma G, Sanduja V (2018) A real time approach to compare PSNR and MSE value of different original images and noise (salt and pepper, speckle, Gaussian) added images. Int J Latest Technol Eng Manage Appl Sci (IJLTEMAS) VII(I):43–46
8. Kumbhakar D, Sanyal K, Karforma S (2021) A secure and efficient authentication in E-commerce. Biosc Biotech Res Comm 14(05):93–99
9. Mathey R, Avadhani PS (2014) An image compression using using discrete cosine transforms and JPEG enconder. IOSR J Comput Eng (IOSR-JCE) 16(2):01–05
10. Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M (2017) CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimed Tools Appl 76(6):8597–8626
11. Prabu RG, Latha K (2020) Ultra secure secret communication by crypto stegano techniques for defence applications. Dogo Rangsang Res J 10 (07)
12. Preedanan W, Kondo T, Bunnun P, Kumazawa I (2018) A comparative study of image quality assessment. IEEE 2018 International Workshop on Advanced Image Technology (IWAIT), (), 1–4. https://doi.org/10.1109/IWAIT.2018.8369657
13. Rabah K (2005) Elliptic curve ElGamal encryption and signature schemes. Inf Technol J 4(3):299–306
14. Sabanoglu T (2021) Global retail e-commerce sales 2014–2024. /https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales (2021). Accessed 20 may, 2021
15. Saleh ME, Aly AA, Omara FA (2016) Data security using cryptography and steganography techniques. (IJACSA) Int J Adv Comput Sci Appl 7(6), 390–397
16. Sara U, Akter M, Uddin MS (2019) Image quality assessment through FSIM, SSIM. MSE and PSNR—A Comparative Study Journal of Computer and Communications 7(3):8–18
17. Thangadurai K, Devi GS (2014) An analysis of LSB based image steganography techniques. International Conference on Computer Communication and Informatics, 03–05
18. Thum C (1984) Measurement of the entropy of an image with application to image focusing. Optica Acta, OPTICA ACTA 31(2):203–211
19. Uky.: E-commerce securities. http://www.uky.edu/~dsianita/390/390wk4.html". Accessed 15 july, 2021
20. Wang Z, Zhao Y, Zhong G (2019) Public-key applications in E-commerce. J Phys Conf Series 1213: 042083. https://doi.org/10.1088/1742-6596/1213/4/042083
21. Zachariah B, Yabuwat PN (2016) Application of steganography and cryptography for secured data communication – a review. Int J Eng Res Technol (IJERT) 5(4):186–190