Ultra-Secure Secret Communication by Crypto Stegano Techniques for Defence Applications

ASHISH SHARMA, NARENDRA MOHAN,

ASHISH SHARMA[1], NARENDRA MOHAN[2]
[1,2]Department of Computer Engineering and Application GLA UNIVERSITY, MATHURA, ashish.sharma@gla.ac.in, narendra.mohan@gla.ac.in

Correspondence:

ASHISH SHARMA
Department of Computer Engineering and Application
GLA UNIVERSITY, MATHURA
ashish.sharma@gla.ac.in

ABSTRACT

This research paper proposes the communication devices in defence sectors shares secret information dynamically and it is vulnerable to hackers as they steal, corrupt or destroy the data. Though existing system uses different cryptographic techniques, yet suffers from various cyber-attacks. In order to communicate secretly, we propose novel optimized crypto stegano system with the cryptographic process implemented by Elgamal cryptosystem with secure key exchange, then steganographic process using quantum LSB image steganography by hiding the encrypted data into the randomly chosen image, also cover image is optimized using eagle strategy particle swarm optimization algorithm for high embedded efficiency. Then the data embedded in image is retrieved using steganographic retrieval technique and it is decrypted at receiver by Elgamal decryption using private key. Based on results, various parameters such as MSE, PSNR, embedded efficiency and carrier capacity are calculated and related with existing methods, thereby higher performance metrics are achieved in our proposed work.

Keywords: Elgamal Cryptosystem, Information Security, Eagle Strategy PSO, Quantum Steganography, Optimization.

DOI: https://doi.org/10.31838/ejmcm.07.02.03

Introduction

Present days information Security is the process of protecting information by using various techniques thus by achieving confidentiality, integrity, availability and non-repudiation. Securing the confidential information is achieved by cryptography, as it provides the high-end security to data by encryption as it transforms the message into the unusable form by various symmetric and asymmetric algorithms using cryptographic keys such as public as well as private keys through various key exchange mechanism. The existing form of cryptosystem ranges from simple key exchange to ultra-level quantum-based pseudo random number generated key exchanges as asymmetric system relies on Diffie Hellman Key exchange mechanism and also password based authenticated key exchange is popular among cryptographic key exchanges, though most are vulnerable to attacks.

In defence communication, the sharing of the secret messages between the transmitter and the receiver is highly confidential task and risk management need to be attained and also the military database such as criminal database needs to be protected from the enemy countries. The military data ranges from small level inter countries arms exchange details to high level Interpol criminal database, where huge amount of big data needs to be processed and it should be stored in the safe environment free from intruders. So, high level of security needs to be provided by using the various cryptographic and steganographic techniques in order to protect the defence communication message sharing as well as protecting our confidential databases.

The existing system in defence communication prevails mainly on the symmetric encryption schemes such as AES, DES, 3DES and it uses the SUITE-B protocols for the secure data transmission. Thus, to improve security mechanism, the proposed methodology uses the two tier of security by clubbing the concept of both advanced high level crypto and stegano techniques to ensure secure transmission and also to protect the military database from enemy countries by embedding on to the image steganography. The level of security may increase the time complexity as well as space complexity of our proposed work, thus we go upon optimization techniques. Here, we use bio inspired optimization process called eagle strategy PSO, an hybrid bio inspired optimization technique, based on two stage iterative process of slow random global search and fast intensive local search to search the best cover blocks of the pixels levels in the image so the encrypted data can be embedded on selected cover blocks of the image efficiently to improve the carrier capacity thus by achieving multi-level of security.

The cryptography technique, we implemented here is Elgamal encryption. The main objective of choosing it is Confidentiality, non-repudiation and integrity. Elgamal encryption is the public key cryptography technique that is used for key generation, encryption and decryption of secret messages. It uses the discrete algorithm problem based on the prime number calculation. Next, steganography technique that we used in quantum LSB steganography that provides good imperceptibility. This technique embeds the two qubits of the secret data on three LSB qubits. The quantum steganography provides high level of embedded capacity, embedded efficiency, carrier capacity, cover image optimization and high level of information security.

The remaining part of this work is as mentioned; Section II implements the technique related to existing cryptography, steganography and optimization techniques for information security and also analyzed with respect to the defence applications. Section III proposes the methodology for the improvements in defence information security with novel optimized crypto stegano model based on various cryptographic and steganographic protocols. Section IV projects the system framework with architectural design for our proposed work. Section V proposes experimental evaluation and performance metrics with comparison with existing methods and Section VI concludes and discusses the future scope this paper.

Existing Models

This part describes and analyses the existing studies of Information security based on various techniques.

Manju Khari et al. [1] in 2019 propose a secure communication based on combination of cryptography and steganography techniques. It uses the EGC encryption method over galois field; a variant of elliptic curve cryptography, based on the discrete logarithmic problem as it reduces the round off error as the message is decrypted only the private key thus by secure key exchange between the sender and receiver then, the matrix XOR steganography for high embedded efficiency by compressing the image into the matrix format before embedding the data and also it optimizes the cover blocks of the image using bio inspired firefly optimization technique. The high embedded efficiency is obtained by using the optimization algorithm by choosing the best position on the cover blocks for embedding operation. The crypto stegano system increases the level of data security. This work has been implemented for secure medical data transmission over IOT network.

Zhiguo Qu et al. [3] in 2018 provides the concept of embedding the secret information on the quantum carrier image to archive high embedded efficiency through matrix coding on both single pixel embedding and multiple pixels embedding and thus high embedding capacity is achieved. Yuling Luo et al. [4] in 2017 provides the image encryption by elliptic curve and chaotic network in which SHA-512 is used for initial value for chaotic system and cross over permutation is done. Then it is embedded by elliptic curve Elgamal encryption based on homo-morphic scheme thus by providing high security. Zichi Wang et al. [6] in 2019 propose the method for secure cover selection for the steganography by resisting pooled Steganalysis. The relation between stegano image and original cover image is calculated for securing the cover blocks of the image for the image steganography.

Junbeom Hur et al. [9] in 2012 provide the concept of disruption tolerant network that allows the devices to communicate by exploring the external nodes. It provides the cryptographic solution based on cipher-text based encryption for the secure wireless network for the military applications. Fang-Yu Rao et al. [14] in 2017 describe the efficiency of the Elgamal encryption in terms of the distributed key generation and decryption of data from plaintext and it resist the brute force attack but suffers from discrete logarithm problem. EM Islas Mendoza et al. [18] in 2013 present the communication scheme for securing messages through LAN, it implements in hybrid cryptosystem by combining the AES-256 for its symmetric encryption and Elgamal for the key encryption. It provides the secure key distribution by Diffie-Hellman protocol. It provides the concept of multi-level encryption methodologies by clubbing private key and public key cryptography.

Hamza Yapici et al. [19] in 2016 worked on the bio inspired optimization process of eagle strategy particle swarm optimization for the power loss minimization application. It has two operations such as random global search as it is slow process and the intensive local search as it is fast computation thus by updating the global best and weight to archive the maximum efficiency. Maninder Kaur et al. [20] in 2017 discussed the comparative case study of various cryptographic algorithms such as DES, 3DES, AES, RSA, Elgamal cryptosystem, Elliptic curve cryptosystem and compared its rounds, key size, block size, security analysis of both symmetric and asymmetric encryption and its merits and demerits are compared for the efficient encryption schemes.

Proposed Model

The proposed approach is split into four modules as encryption by Elgamal cryptosystem, optimization by eagle strategy particle swarm optimization, steganography by quantum LSB image steganography and decryption by Elgamal cryptosystem.

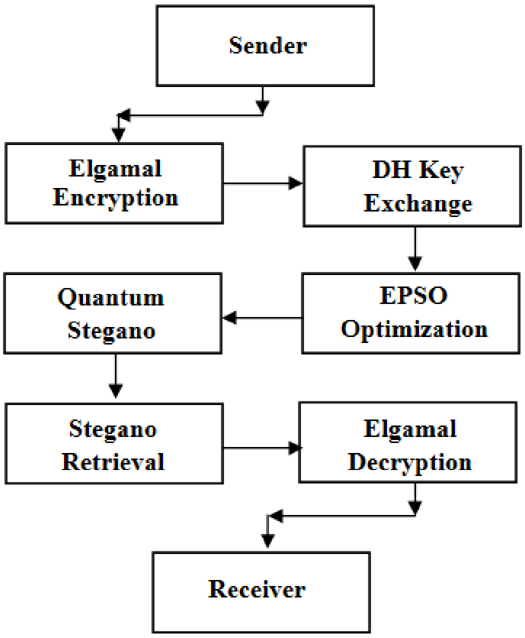


Fig.1 System Block Diagram

A. Elgamal Encryption

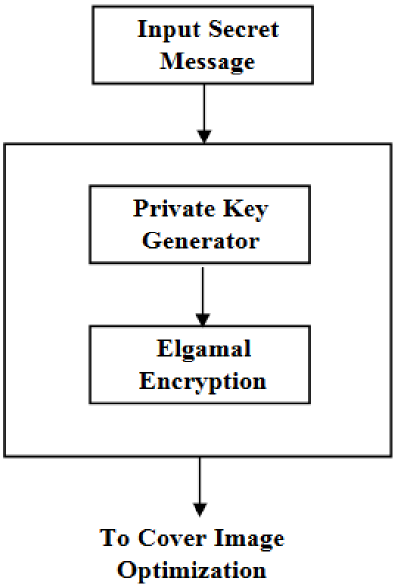


Fig.2 Encryption Block Diagram

Encryption is the process at the sender in the cryptography to convert the original message into unusable form for secure data transfer. In our proposed work we used Homomorphic encryption scheme called Elgamal Encryption Elgamal Cryptosystem consists of two parts as key generation and encryption part and key exchange is done using the key exchange by Diffie-Hellman process. It is Public key encryption scheme which uses the private key at the receiver.

1) Key Generation

Step1: At first choose a, the prime number of high value and β, the prime root of a.

Step 2: Choose I, the random generated integer in the range of 1 < I < a-1.

Step 3: Calculate the P as m^I mod a.

Step 4: Generate the Private Key: I and the Public Key: {a, β, P}.

2) Encryption

Step 1: Characterize the initial sender message as an integer t, such that 0 ≤ t ≤ a-1.

Step 2: Then, select random integer N in range 1 ≤ N ≤ q-1.

Step 3: Calculate the key generated one time, K = P^N mod a.

Step 4: Lastly, Encrypt message t as integer's pairs (C_1, C_2) where C_1=m^N mod a, C_2 = K.t mod a

B. Optimization

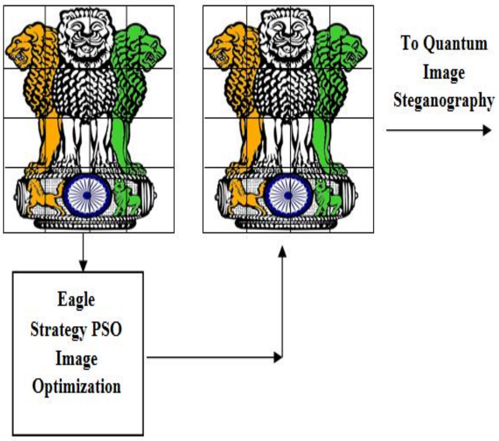

To Quantum Image Steganography
Eagle Strategy PSO Image Optimization

Fig.3 Optimization block diagram

Optimization helps to minimize the time complexity and space complexity also by improving the carrier capacity and embedded efficiency. In our proposed work, we choose bio inspired optimization called as Eagle Strategy Particle Swarm Optimization for optimizing the randomly chosen the best pixels in the cover blocks of the color image for the encrypted data after encryption part to be embedded on the color image using optimized strategy to achieve high embedded efficiency.

1) Eagle Strategy Particle Swarm Optimization

Step 1: Initialize the objective function as f(x).

Step 2: Initialize the randomly generated population (at t=0).

Step 3: Then, while (||min f (t+1) - min f (t) || ≤ tolerance or t> maximum number of iterations)

Perform global slow search randomly by (Levy walks) X^{t+1} = X^t +αL (s,ƛ), (ƛ=1.50, α=1.00, and the step length set as 5)

Then search for promising solutions.

Step 4: Determine the randomly generated number and initialize the switch parameter s to control between the local fast search and the global slow search.

If (s<random)

Switch to the local intensive fast search (go to 5).

Other wise

Toggle to the global slow search (go to 6).

Step 5: In the fast-intensive local search process, find for the hopeful solution. Determine latest position and velocity of each particle through 5 & 6,

Step 6: After that estimate the new fitness (based on objective function calculation from tolerance levels as given input by Newton-Raphson Image Optimization).

If p (u_i (t+1) <p (position-best$_i$ (t))

(Position- best$_i$ (t+1)) = u_i (t+1)

Update,

T=t+1

Step 7: for the stopping condition,

Greatest iterations number or tolerance level (based on input)

Step 8: while for given condition is provided, then terminate the optimization process or else move to step 3.

C. Quantum Steganography

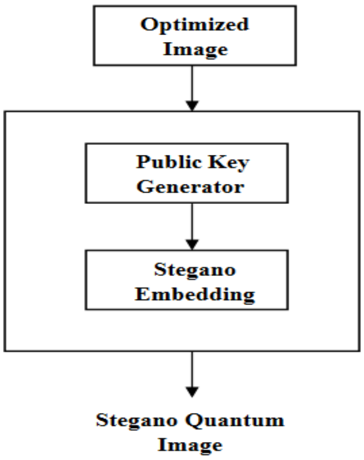


Fig.4. Stegano Block Diagram

Steganography is technique of masking, hiding or embedding the secret information on the images, videos, audios for secure communication. Steganography is mainly used for Military applications. In our proposed system, we combine the cryptography and steganography process and we implement quantum steganography based on matrix coding process by least significant bit embedding on the quantum bits. It is implemented by single pixel embedding process and also the high embedded capacity in order to rectify the quantum noise and eve attacks.

1) Stegano Encoding

Single Pixel Embedding (1, 3, 2) stegano coding technique masks the two qubits onto the three Least Significant Quantum bits is encoded based on three color channels by RGB as Red, Green, Blue in the single pixel. The elaborated steps of Single Pixel Embedding (1, 3, 2) are implemented as follows.

Step 1: The Original image in terms of the Novel quantum representation of digital color images represented as RGB image of size $2^n * 2^n$ can be expressed as (1).

$$|O|= \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} \begin{pmatrix} |R_7^i\ R_6^i\ R_0^i|_{1-8} \lceil G_7^i\ G_6^i\ G_0^i \rceil_{9-16} \\ |B_7^i\ B_6^i\ B_0^i|_{17-26} \langle i \rangle \end{pmatrix} \quad (1)$$

The i^{th} pixel in image of quantum color original image |O| as by RGB representation has three Least Significant Quantum bits, i.e., $(R_0^{i'})_8(G_0^{i'})_{16}(B_0^{i'})_{24}$

Step2: Then, the 2_{ith} quantum bit $|X_{2i}|$ and $(2i + 1)^{th}$ quantum bit $|X_{2i+1}|$ is encoded into the $(R_0^{i'})_8(G_0^{i'})_{16}(B_0^{i'})_{24}$ by (1, 3, 2) coding. After encoding the secret messages into corresponding pixels based on two bits by iteratively preceding this quantum LSB method, quantum Original image |O| becomes the stego image |S|.

$$|S|= \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} \begin{pmatrix} |R_7^i\ R_6^i\ R_0^i|_{1-8}\ \lceil G_7^i\ G_6^i\ G_0^i \rceil_{9-16} \\ |B_7^i\ B_6^i\ B_0^i|_{17-26} \langle i \rangle \end{pmatrix} \quad (2)$$

By recursively implementing this process, the encoding process is finished.

2) Stegano Decoding

Step 1: Stegano image is the vector of complex form in Space denoted by Hilbert of size 2^{24+n}. Then decode the vector S into straight product of the RGB pixel as illustrated by quantum color of Red, Green and Blue for the data and the corresponding information with respect to position is given as (3)

$$S = m_0 * \begin{pmatrix} 1 \\ 0 \\ \cdot \\ 0 \end{pmatrix}_{2^{2n} * 1} + m_1 * \begin{pmatrix} 0 \\ 1 \\ \cdot \\ 0 \end{pmatrix}_{2^{2n} * 1} + \ldots + m_2{}^{2n-1} * \begin{pmatrix} 0 \\ 0 \\ \cdot \\ 1 \end{pmatrix}_{2^{2n} * 1}$$

(3)

Step 2: All pixels' RGB information of the m_0, m_1, ... , $m_2{}^{2n}{}_{-2}$, $m_2{}^{2n}{}_{-1}$are encoded with respect to binary sequence that contains 24 qubits. Afterwards, the 8th quantum bit, the 16th quantum bit, the 24th quantum bit of the i^{th} pixel's in the binary sequence are recovered to get$(R_0^{i'})_8(G_0^{i'})_{16}(B_0^{i'})_{24}$. In same way all of the red, green, blue, $(R_0^{i'})_8(G_0^{i'})_{16}(B_0^{i'})_{24}$, $(R_0^{2^{2n}-1})_8(G_0^{2^{2n}-1})_{16}(B_0^{2^{2n}-1})_{24}$ also get. These values form the binary string with the initial length as 3×2^{2n}.

Step 3: Each of the three quantum bits of the binary strings are combined to retrieve the two secret quantum bits by (1, 3, 2) encoding. By this way, the new string of length 2^{2n+1} is formed. With respect to secret information length, the unneeded part of a new string is removed to get final string of secret information from quantum images. By this retrieval process is also completed.

The steganography provides the data hiding on the pixel of least intensity by multi pixel embedding. Thus, by using the public keys the retrieval of the information embedded can be obtained at the receiver thus by enhancing security.

System Architecture

System framework has 4 components as follows,

A. Encryption

The sender sends the highly confidential secret messages or database through internet by secure communication methods. At first the secret message is encrypted using the Elgamal encryption. It is Homomorphic encryption process, probabilistic based, random, stochastic, asymmetric method, uses the public key cryptography. The Elgamal method generates the random key and it encrypts the original message by the public key at the transmitter. It also generates the private key in the key generation, so that there is no sharing of key in public key cryptography as it uses the private key at the receiver side and it has high security as compared to symmetric encryption. The secure key exchange is done by Diffie-Hellman process by sharing the key securely. Then the output of the Elgamal encryption is the cipher text or encrypted data that need to be send to the next phase.

B. Optimization

After encrypting the secret message using asymmetric Elgamal encryption, the cover image is chosen at the random, after choosing the cover image, the optimization of the cover blocks of the image is done by using the bio inspired optimization process called Eagle Strategy Particle Swarm Optimization. It is the hybrid algorithm, two stage iterative processes that is mainly used for image processing optimization problems such as searing the best fit in the pixels of the image for embedded operations. It has meta-heuristic process by using global search and local search. Global search is random and local search is intense to find the optimal cover block that suits the requirement for archiving the higher embedded efficiency and the optimized cover image is send to the steganography process.

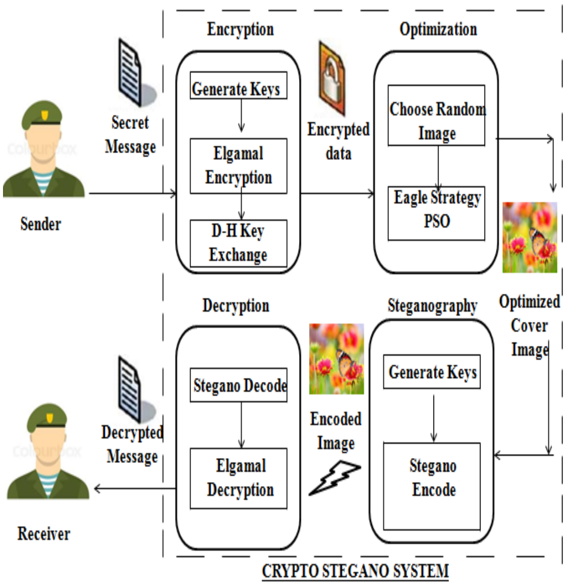


Fig.6. Architectural Diagram

C. Steganography

The Steganography is art of hiding the useful information by watermarking. The combination of crypto Stegano makes the system high secure. In our proposed work, we used the Quantum LSB Steganography that embeds 2 secret qubits on to 3 LSB quantum blocks by single pixel embedding technique and mostly only one LSQ bits would be changed. This method provides the noteworthy research areas of the Quantum communication. It has high embedded efficiency of matrix coding as well as high embedded capacity. After the embed process, all the confidential information, with correspond to implement this process, the quantum image in color form becomes the quantum image in stegano form with information embedded. It generates the key by Elgamal technique at the encoding operation and key is shared to the decoder part. Finally, the Stego image is sender from the sender to the receiver through wireless network.

D. Decryption

At the receiver, the decryption part is done. Before decryption the decoding or extraction of the embedded data from the stego image is done by using public key. Qu bits are extracted from the image by converting the pixel RGB information into the binary strings and the 2 secret qubits are extracted from the 3 LSQ bits to obtain the final binary strings of the embedded data and binary strings are converted into original embedded data. Then the embedded data is decoded at receiver by using the key as by private based on the Elgamal decryption to obtain the secret message that the sender had transmitted.

Results and Analysis

The Eclipse Integrated Development Environment (IDE) with the PyDev plug-in is simulated for the execution of the proposed process. The language used is Python. Software descriptions are Python 3.7, Eclipse Neon, PIP 1.3.1 (Python package installer), various image processing packages, cryptography, steganography, optimization packages and Matlab package such as matpyplot is used for visualization of the data.

A. Data Description

The input data that we have used are of user defined choice of the finite length of messages. The messages can be of any length depending upon the user requirements. The set of Images are collected, so that the sender can randomly choose the image from set for the steganography operation. The user input has the secret messages in the form of string data type and it is converted into ASCII value for processing.

B. Parameter Calculation

To project the efficiency, scalability and robustness of proposed Elgamal based Quantum Steganography system, Mean Square Error of the system is evaluated with Peak Signal to Noise Ratio and in addition with Embedded Efficiency and Carrier Capacity. These results are compared to tested methods such as Elliptic Galois Cryptography (EGC), Flexible Macro Block Ordering (FMO). Optimized Modified Matrix Coding (OMMC), Least Significant Bit (LSB) embedding. Various bar charts have been shown to compare the proposed techniques with the existing techniques. The performance metrics is calculated by,

1) Mean Square Error:

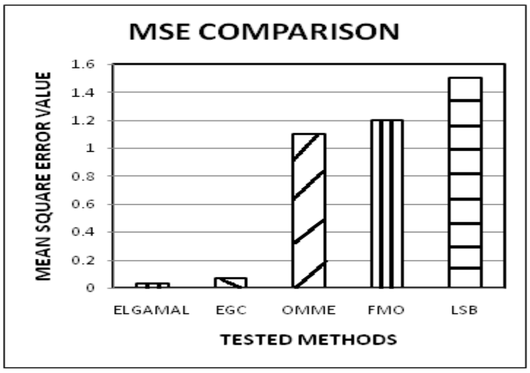


Fig.7. Mean Square Error Comparison

It correlates and finds the relation between the images, thus by the calculating similarity in image and distortion range in image and it provides room for the estimation of the reliability.

Mean Square Error = $\frac{1}{\mathrm{N}}\sum_{i=A,B}^{n}(A-B)^2$(4)

N is the total amount of pixels in image, A is Original image, and B is final Stegano image.

2) Peak Signal to Noise Ratio:

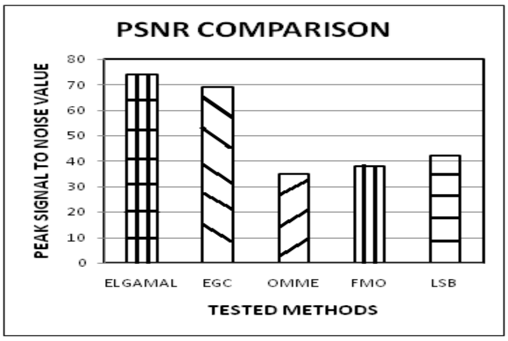


Fig.8. Peak Signal to Noise Ratio Comparison

PSNR is calculated by the invisibility of stegano image. It can be used for both dynamic as well as static images

Peak Signal to Noise Ratio = 10log$_{10}$ $\frac{255^2}{\text{Mean Square Error}}$(5)

3) Embedding Efficiency:

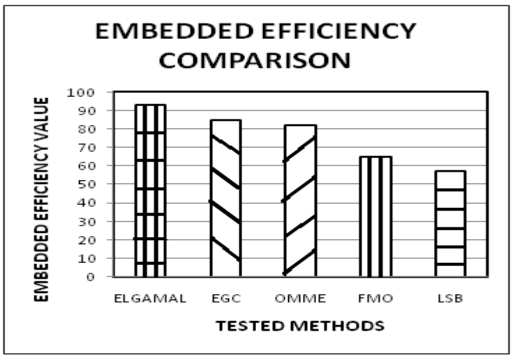


Fig.9 Embedded Efficiency Comparison

It is the range of quantity of secrets bits embedded in cover block, which denotes the efficiency of embedding process. Effectiveness is calculated by

Embedded Efficiency = $\frac{a+1}{a}$ n (6)

Where a is bit to be embedded in the cover block of the image and n is the total amount of secret bits in embedding technique.

4) Carrier Capacity:

It is the total capacity of the system to mask encoded information within the cover block. The quantity of its capacity value is directly proportional to its processing performance.

Carrier Capacity = $\frac{Total\ number\ of\ secret\ bits}{Number\ of\ bits\ in\ the\ cover\ block}$(7)

Carrier capacity is used to hide capacity of data in carrier cover and estimated in range of bits per pixel.

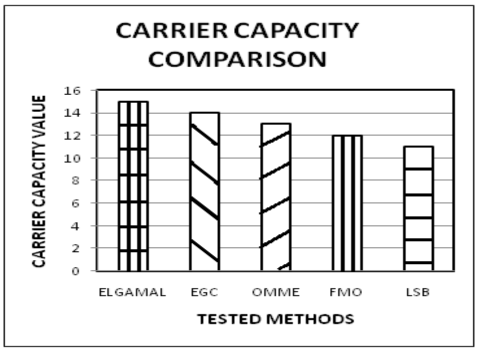


Fig.10. Carrier Capacity Comparison

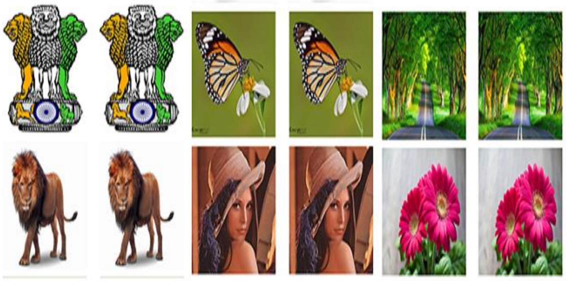


Fig.11. Sample images of original vs stegano images (from top to bottom – Emblem, Lion, Butterfly, Lena, Nature, Flower)

S.No.	Name	PSNR	MSE	Carrier Capacity	Embedded Efficiency
1	Emblem	75.337	0.0019	16.314	94.716
2	Lion	74.305	0.0024	12.351	94.231
3	Butterfly	74.407	0.0023	16.837	93.421
4	Lena	76.374	0.0014	14.065	95.274
5	Nature	76.022	0.0016	15.063	90.695
6	Flower	75.689	0.0017	17.464	94.633

Table.1. Performance metrics of sample images

The Elgamal protocol provides good performance on various performance metrics as compared to existing techniques. Performance metrics are calculated with respect to existing techniques such as LSB, FMO, OMME and EGC. The MSE of proposed protocol is comparatively small as compared to existing methodology (0.001, 0.002, 1.10, 1.25 and 1.51). The proposed method provides good PSNR as compared to existing techniques (74.10, 71.45, 31.25, 38.50 and 46.25). The proposed method provides high embedding efficiency performance as compared to existing embedding techniques (93.00, 86.50, 85.00, 68.25 and 56.25) thus providing superior performance, respectively. It has carrier capacity compared by (15.0, 14.1, 13.9, 12.0 and 11.0) as it can be improvised by optimization process.

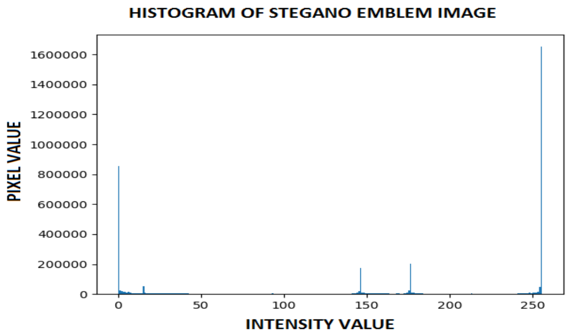


Fig.12. Histogram of Emblem image

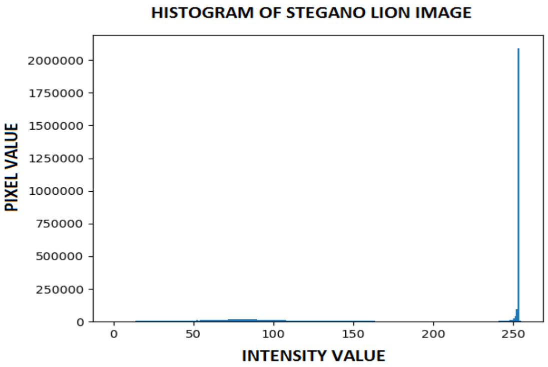
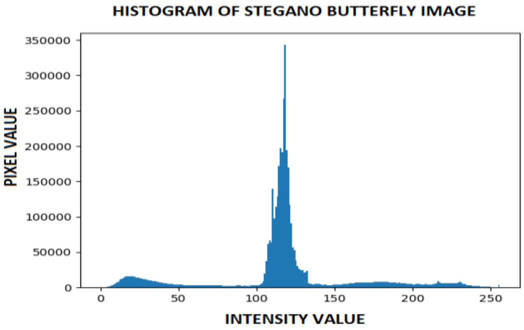
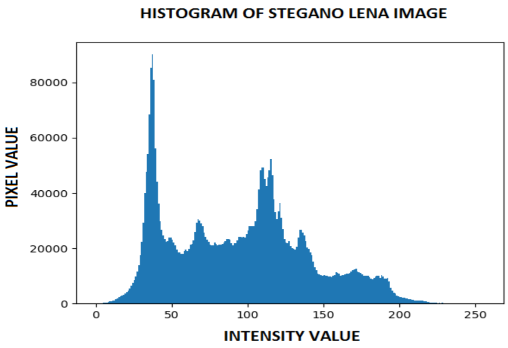


Fig.13. Histogram of Lion image



Figurre.14. Histogram of butterfly image



e

Fig.15. Histogram of Lena image

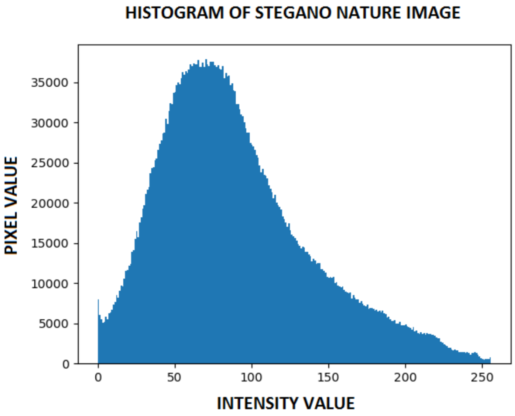


Fig.16. Histogram of Nature image

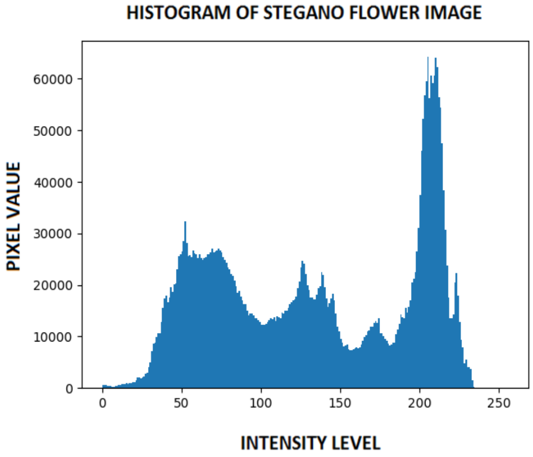


Fig.17. Histogram of Flower image

In this work, sample of six images such as Indian emblem image, lion image, butterfly image, Lena image, nature image and flower image have been taken and its performance metrics is analyzed and its histogram graph is plotted for the understanding of the embedding the encrypted data on the cover blocks within the image for the bits per pixel intensity levels with respect to number of pixels. The histogram is plotted by intensity levels with respect to the pixel values. The images are resized to 2000*2000 pixels so that equal pixel embedding is possible. Therefore, the proposed techniques are highly optimized, robust, stable, confidential and secure. The proposed methods provide the high level of security and it is free from most of the cyber attacks. It provided good results as compared to existing methodologies and it also provides the novelty of the system design by incorporating the combination of crypto and stegano with addition to the optimization process. In this work, the three main algorithms have been implemented. The first algorithm is Elgamal cryptosystem with secure key exchange and key generation. Next is quantum least significant bit image steganography for the stegano operation. At last, the bio inspired optimization process called eagle strategy particle swarm optimization, this is useful for choosing the best position on the cover blocks of the image for the best embedding in the quantum color images. This combination is novel and its design implementation provides high efficiency and robustness as compared to the existing system. Thus, higher performance metrics are obtained in this proposed work.

Conclusion

In this proposed work, we have presented the novel implementation of hybrid crypto stegano system that combines the crypto and stegano techniques. Asymmetric based Elgamal cryptography that we implemented provides the high level of information security during the transmission of the secret messages; also secure key exchange provided for the improved security. It also provides information hiding through the advanced embedded efficient method by quantum steganography technique. With the help of eagle strategy particle swarm optimization, the huge amount of information can be securely transferred over the wireless medium by choosing the best position of pixels in image for embedding the secret data on the cover blocks of image. The proposed work is implemented in the Eclipse IDE with PyDev plug-in by using python language with pip packages for image processing and various cryptographic and steganographic packages has been utilized for optimized crypto stegano implementation. Performance metrics are analyzed by various performance metrics parameters and are calculated and compared with the existing methods thus higher performance metrics are achieved in our proposed work.We can extend the work with number of directions our work can potentially take in the future. We have implemented Elgamal cryptosystem, but due to rapid advancement of quantum computing, the post quantum cryptography will be uptake the future cryptography. The stegano methods will rely mainly on artificial intelligence for future computing and optimization techniques will be focusing mainly on hybridization techniques to tackle the quantum computing for the various applications in cyber security.

References

[1] Manju Khari, Aditya Kumar Garg, Amir H. Gandomi , Rizwan Patan and Balamurugan Balusamy, “Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques”, IEEE Transactions on Systems, Man, and Cybernetics, pp. 1-8, Feb. 2019.

[2] Inaam Rabah Mohammad, Dr.Ziyad Tariq Mustafa, “Image Steganography based on behaviour of the Particle Swarm Optimization”, Journal of Theoretical and Applied Information Technology, pp. 3696-3706, 2018.

[3] Zhenwen Cheng , Zhiguo Qu and Xiao jun Wang, “Matrix Coding Based on Quantum Image Steganography Algorithms”, IEEE Access, pp. 1-15, 2018.

[4] Yuling Luo, Xue Ouyang, Junxiu Liu and Lvchen Cao, “An image encryption method based on elliptic curve ElGamal encryption and chaotic systems”, IEEE Access, pp. 1-17, 2017.

[5] Zhengyan Li, Gang Xu, Zhiguo Qu, Xiaojun Wang and Shengyao wu, “Quantum Steganography Protocol Based on the Quantum Expansion and the Grover Algorithm”, IEEE Access, pp. 50849-50557, 2019.

[6] Zichi Wang and Xinpeng Zhang, “Secure Cover Selection for Steganography”, IEEE Access, pp. 1-11, 2019.

[7] Warley Gramacho da Silva, Rafael Lima de Carvalho, Ary Henrique Oliveira de Morais, “Optimizing the Image Steganography based on Particle Swarm Optimization Algorithm”, International Journal of the Computer Application, pp. 1-5, 2017.

[8] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, M. Shamim Hossain, Samir Elmougy and Ahmed Ghoniem, “Secure image quantum steganography for the fog cloud IOT”, IEEE Access, pp. 1-8, 2018.

[9] Junbeom Hur and Kyungtae Kang, “Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks”, IEEE/ACM Transactions on Networking, pp. 1-11, 2012.

[10] Tesfay Gebreslassie, Dr. T.Pandikumar, “Information Security by Image based Steganography”, International Journal of Engineering and Technology, pp. 2839-2844, 2016.

[11] M. Soleimanpour, S. Talebi and H. Azadi-Motlagh, “Novel Technique of Steganography based on the Genetic Algorithm in the Spatial Domain”, Iranian Journal of Electronic Engineering, pp. 67-76, 2013.

[12] Ruimin Jia, Dengxu He, “Artificial Bee Colony Algorithm with Two-Stage Eagle Strategy”, Ninth International Conference on Computational Intelligence and Security, pp. 16-21, 2013.

[13] S. R. Jino Ramson, K. Lova Raju, S. Vishnu and Theodoros Anagnostopoulos, “Nature Inspired Optimization Techniques for Image Processing— A Short Review”, Nature Inspired Optimization Techniques for Image Processing Applications, Intelligent Systems, pp. 113-143, 2019.

[14] Fang-Yu Rao, “On the Security of a Variant of ElGamal Encryption Scheme”, IEEE Transactions on Dependable and Secure Computing, pp. 1-4, 2017.

[15] Xin-She Yang, Suash Deb, Tatisilwai Xingshi He, “Eagle Strategy with Flower Algorithm”, IEEE Access, pp. 1213-1217, 2013.

[16] M Soleimanpour, S. Talebi and H Azadi Motlagh, “A Novel Technique for steganography method based on Improved Genetic Algorithm in spatial domain”, International Journal of Electrical and Electronics Engineering, pp.67-76, 2013.

[17] Fei Peng, Xiang Zhang, and Min Long, “Robust Coverless Steganography based on the LDA and DCT Topic Classification”, IEEE Transactions on Multimedia, pp. 1-16 2018.

[18] EM Islas Mendoza, CA Jimenez Vazquez, VM Silva Garcia, R Flores Carapia, “Diffie-Hellman Protocol based on Elgamal and AES cryptosystems”, IOSR Journal of Engineering, pp. 30-33, 2013.

[19] Hamza Yapici and Nurettin Cetinkaya, “An Improved Particle Swarm Optimization Algorithm using Eagle Strategy for Power Loss Minimization”, Hindawi, pp. 1-11, 2016.

[20] Maninder Kaur, Navpreet Kaur and Baldeep Singh “Comparative study of different cryptographic

Algorithms”, International Journal of Advanced Research in Computer Science, pp. 352

[21] Kumar, R., Bhardwaj, D., Mishra, M.K. 2020. Enhance the Lifespan of Underwater Sensor Network through Energy Efficient Hybrid Data Communication Scheme 2020 International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control, PARC 2020 9087026, pp. 355-359

[22] Kumar, R., Bhardwaj, D. 2020. An improved moth-flame optimization algorithm based clustering algorithm for VANETs Test Engineering and Management 82(1-2), pp. 27-35

[23] Bhardwaj, D., Chaturvedi, A. 2020. A Hybrid Resource Optimization Technique using Improved Fuzzy Logic Guided Genetic Algorithm for 5G VANETs Test Engineering and Management 82(1-2), pp. 36-44

[24] Kumar, M., Bhardwaj, D.2019 Optimized cluster head and secret key comparison based secure routing in WSN Journal of Advanced Research in Dynamical and Control Systems 11(11 Special Issue), pp. 183-188

[25] Agarwal, R., Jalal, A. S.,Agrawal, S.C. Arya, K. V,’ Fake and Live Fingerprint Detection Using Local Diagonal Extrema Pattern and Local Phase Quantization’. International Conference on Deep Learning, Artificial Intelligence and Robotics, (ICDLAIR) 2019'. MNIT JAIPUR, December 07-08, 2019 (Scopus Indexed)

[26] Agarwal, R., Jalal, A. S.,’ Efficient Document Classification using Phrases Generated by Semi-Supervised Hierarchical Latent Dirichlet Allocation.’ International Journal of Engineering Research in Computer Science and Engineering, NIT, Uttrakahnd:2018.

[27] Agarwal, R., Arya, K., & Shekhar, S. (2010, July). An architectural framework for web information retrieval based on user's navigational pattern. In 2010 5th International Conference on Industrial and Information Systems (pp. 195-200). IEEE.

[28] Agarwal, R., Arya, K. V., Shekhar, S., & Kumar, R. (2011, October). An Efficient Weighted Algorithm for Web Information Retrieval System. In 2011 International Conference on Computational Intelligence and Communication Networks (pp. 126-131). IEEE.

[29] Varun K L Srivastava, N. Chandra Sekhar Reddy, Dr. Anubha Shrivastava, "An efficient Software Source Code Metrics for Implementing for Software quality analysis", International Journal of Emerging Trends in Engineering Research, Volume 7, No. 9 September 2019.