A Multilevel Secured Mechanism for Data Protection

Anjali Malik, Sunil Jadav, and Shailender Gupta

1 Introduction

With the advancements in the technology, there is a significant role of information security in our day-to-day life. The advancements in technologies have forced to develop secure mechanism for data communication. So, to provide data security, cryptography and steganography mechanisms are used. Cryptography converts the data from one form to another that is not understood by the intruder [1]. The data sent through this process is in unreadable form so that if any unauthorized user has access to it, it still can't understand. This mechanism involves encryption and decryption processes.

Steganography is the process in which the user hides the data into text files, audio, video or an image [2].

The intruders can expose the data, alter the data or may distort the data. But steganography or cryptography alone fails to provide security to the data. However, the combination of the two is a more reliable and strong mechanism. So to solve this problem, the cryptography and steganography mechanisms are used in combination. The data is first encrypted using the encryption process and then it is embedded into an image. Figure 1 shows the basic block diagram of the multilevel security mechanism.

The combination of the two mechanisms improves the overall security of the system as well as fulfill some desirable features such as memory usage, security and strength for sensitive information transmission across an open channel.

This paper proposes a multilevel security mechanism for data communication by involving both cryptography and steganography mechanisms to incorporate high-level security to the data and for large-area applications. Also, we have incorporated

A. Malik (✉) · S. Jadav · S. Gupta
J.C, Bose University of Science and Technology, YMCA, Faridabad 121006, India
e-mail: anjalimalik@jcboseust.ac.in

P. Singhal et al. (eds.), *Recent Developments in Electrical and Electronics Engineering*,
Lecture Notes in Electrical Engineering 979,
https://doi.org/10.1007/978-981-19-7993-4_16

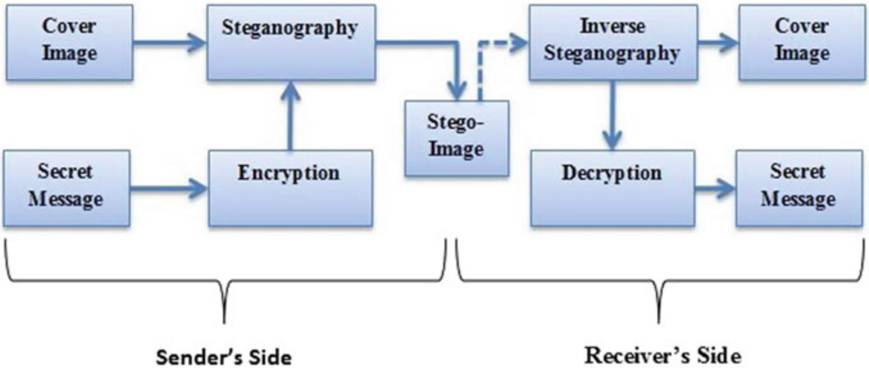


Fig. 1 Basic block diagram of multilevel security mechanism

Huffman compression to enhance the security as well as to increase the data embedding capacity. The data is first encrypted using a qubit encryption mechanism. It is then compressed using Huffman compression for embedding in the cover image. The rest of the paper is organized as follows: Sect. 2 gives the literature survey. The proposed mechanism is shown in Sect. 3. Section 4 provides the setup parameters. A thorough analysis of results is done in Sect. 5 followed by conclusion and references.

2 Literature Survey

Table 1 given below provides the literature survey used till date.

Table 1 shows that the various multilevel techniques available in the literature use various encryption and steganography mechanisms to enhance the security of the data. But very few techniques use compression techniques in their proposed mechanism. Also, very few researchers have worked on the pseudo random LSB approach to embed the data in an image. Thus, our proposed technique aims not only at increasing the embedding capacity but also at securing the data to great extent.

3 Proposed Mechanism

The proposed mechanism involves three stages: Encryption, Compression and Embedding.

Encryption

Figure 2 shows the detailed encryption process used in the proposed mechanism. It involves substitution, permutation and diffusion processes. Each of them involves

Table 1 Literature survey

Proposed by	Cryptography technique used	Steganography technique Used	Compression
Masud Karim et al. [3]	Encryption using secret key	Modified LSB	Huffman compression
Gokul et al. [4]	Visual cryptography	LSB (Least significant Bit)	–
Shailender Gupta et al. [5]	RSA + Diffie Hellman	LSB	–
Mohammad et al. [6]	Diffie Hellman	LSB	–
Nivedhitha et al. [7]	DES	LSB	–
Ramakrishna Mathe et al. [8]	Diffie Hellman	LSB	–
Md. Rashedul Islam et al. [9]	AES	LSB using Status bit	–
Aung et al. [10]	AES	DCT	–
Shingote Parshuram et al. [11]	AES	LSB	–
Sangeeta Dhall et al. [12]	Vigenere	Pseudo random LSB	Huffman compression
Mohamed Elhoseny et al. [13]	AES + RSA	DWT	–
Ashraful Tauhid et al. [14]	AES	LSB + DWT	–
Nabanita Mukherjee et al. [15]	Dynamic Pairing function	PVD (Pixel Value Difference)	–

the use of a key generated from the quantum logistic map to make the encryption key-dependent process for a highly secured mechanism.

The quantum chaotic map with the lowest order quantum corrections is followed [15]. The x(i), y(i) and z(i) values are taken as keys to make the encryption process unique. Even for single bit of change in key or initial conditions makes up a unique encryption process.

The data is passed through the substitution block where the values of the data are replaced with the new values using a dictionary. The dictionary contains a new value for possible values which is dependent on the key. For different keys, the dictionary to be used is unique. Then the substituted data is passed to the permutation block, where the data is shuffled. The unique positions at which data is to be shuffled are generated for the key. Then the shuffled data is further changed in the diffusion block. In this block, the data is XORed with the sequence of key of the same size as of data to get the encrypted data.

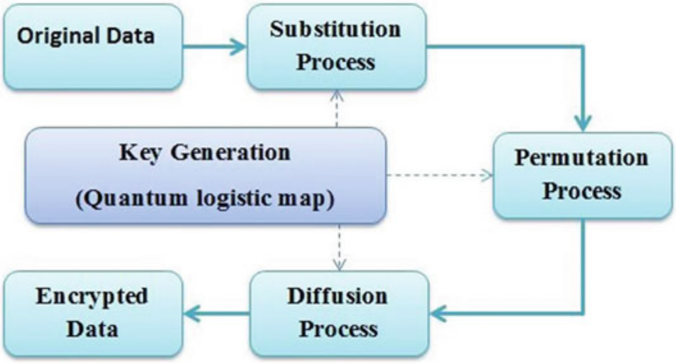


Fig. 2 Block diagram of encryption process used in proposed security mechanism

SUBSTITUTION PROCESS

```
Input: a=original data; anew= substituted data
[m n]= size(a);
s=uint16(randperm(256));
s=s(1:256)-1;
%s(256)=0;
for i=1:1:m
    for j=1:1:n
        b=a(i,j);
        anew(i,j)=s(b+1);

    end
  end
```

PERMUTATION PROCESS

```
Input:ip=randperm(length(anew); ip1= permuted data
for(i=1:length(anew))
        b1=ip(i);
        ip1(b1)=anew(i);
end
```

DIFFUSION PROCESS

```
Input:X2=(randi([0,255], length(a))); diff= diffused data
for(i=1:1:length(a))
    diff(i)=bitxor(ip1(i),X2(i));
end
```

Compression

Now to further increase the security of the mechanism and also to increase the embedding capacity as faced by other researchers available in the literature, data is compressed. The Huffman compression is used to compress the data as it requires less storage space and its lossless behavior [16].

The compressed data is now to be embedded in the cover image.

Embedding

Figure 3 shows the detailed embedding process used in the proposed mechanism.

Now for the embedding process first the edges present in the image are detected. This is due to the fact that the change in data of the edges cannot be visually detected.

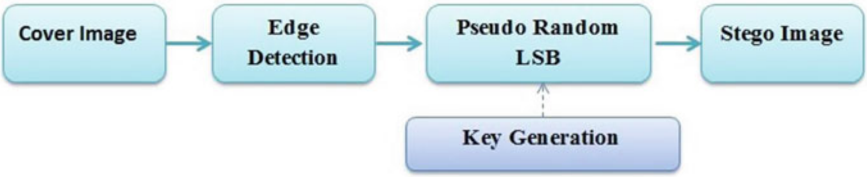
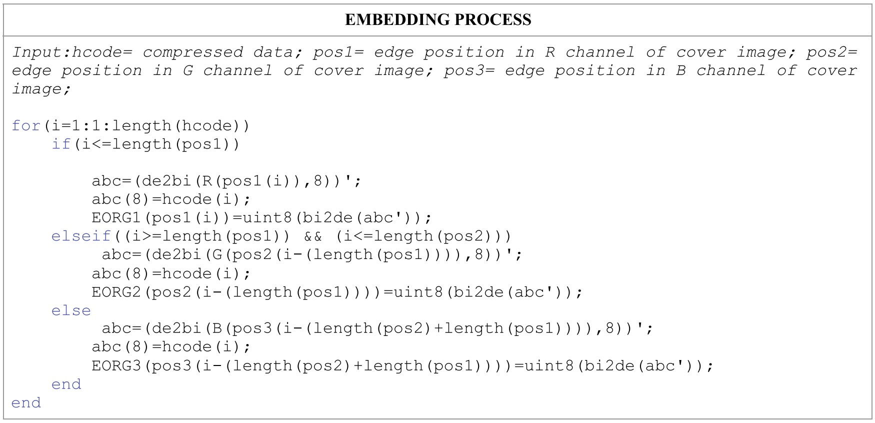


Fig. 3 Block diagram of embedding process used in proposed security mechanism

The edges are detected using the canny edge detection filter. This improves the anti-noise ability and keeps the edge image more clearly [17].

The position of edges is detected where the data in the LSB of the pixels need to be embedded. The positions are scrambled using the quantum map to make the data scrambled and increase the security of data. The data is then embedded in the LSB positions of the edges randomly.

The process to retrieve the data at the receiver's end is just the reverse of the encryption process.



EMBEDDING PROCESS

Input:hcode= compressed data; pos1= edge position in R channel of cover image; pos2= edge position in G channel of cover image; pos3= edge position in B channel of cover image;

```
for(i=1:1:length(hcode))
    if(i<=length(pos1))

        abc=(de2bi(R(pos1(i)),8))';
        abc(8)=hcode(i);
        EORG1(pos1(i))=uint8(bi2de(abc'));
    elseif((i>=length(pos1)) && (i<=length(pos2)))
         abc=(de2bi(G(pos2(i-(length(pos1)))),8))';
        abc(8)=hcode(i);
        EORG2(pos2(i-(length(pos1))))=uint8(bi2de(abc'));
    else
         abc=(de2bi(B(pos3(i-(length(pos2)+length(pos1)))),8))';
        abc(8)=hcode(i);
        EORG3(pos3(i-(length(pos2)+length(pos1))))=uint8(bi2de(abc'));
    end
end
```

4 Setup Parameters

Table 2 provides simulation setup parameters used, while performing different experiments using the proposed mechanism.

Table 2 Simulation setup parameters

Processor	1.50 GHz Intel Core i3
Operating system	Windows 8
Image type	.jpg,.jpeg
Simulation tool	MATLAB version: R2014a serial update 2
Image type	RGB

5 Result

The MATLAB version R2014a software is used to simulate all the results. The simulation results of the proposed mechanism demonstrated below are the average for 10 different images for the below-mentioned performance matrices:

Visual Perceptibility Analysis

For the desired multilevel security mechanism, the distortions introduced in the cover image because of the data embedding process must not be recognized by human eyes as shown in Fig. 4.

It can be observed from Fig. 4 that the proposed technique does not show a perceivable change in the image.

Quantitative Analysis

The embedding process introduces distortion and noise in the cover image. It is essential to measure quantitative measures related to the quality.

Bit Error Rate (BER): For desirable mechanism, BER must be low [15]. Table 3 provides the BER of the proposed technique to the other techniques available in the literature.

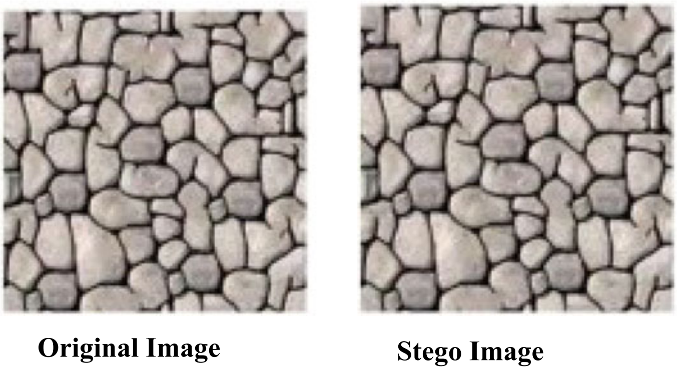


Fig. 4 Visual perceptibility of the proposed technique

Table 3 BER of the proposed technique to the other techniques available in the literature

References	BER
[14]	1.54
[15]	1.47
Proposed	0.01019

Table 4 MSE of the proposed technique to the other techniques available in the literature

References	MSE
[14]	0.0339
[15]	2.08
Proposed	3.067

Mean Square Error (MSE): For a desirable mechanism, MSE value must be low [15]. Table 4 provides the MSE of the proposed technique to the other techniques available in the literature.

Peak Signal to Noise Ratio (PSNR): For a desirable mechanism, PSNR must be high [15]. Table 5 provides the PSNR of the proposed technique to the other techniques available in the literature.

Universal Image Quality Index (UIQI): For a desirable mechanism, UIQI must be close to 1 showing similarity in the cover image and corresponding stego image [15]. Table 6 provides the UIQI of the proposed technique to the other techniques available in the literature.

Structural Similarity Index Metric (SSIM): For a desirable mechanism, SSIM must be close to 1 showing similarity in the cover image and corresponding stego image [15]. Table 7 provides the SSIM of the proposed technique to the other techniques available in the literature.

Table 5 PSNR of the proposed technique to the other techniques available in the literature

References	PSNR (dB)
[14]	62.89
[15]	41.59
Proposed	55.66

Table 6 UIQI of the proposed technique to the other techniques available in the literature

References	UIQI
[14]	0.9054
[15]	0.9663
Proposed	0.9857

Table 7 SSIM of the proposed technique to the other techniques available in the literature

References	SSIM
[14]	0.93415
[15]	0.9972
Proposed	0.9985

6 Conclusion

In the proposed model, we have incorporated an encryption process which involves key-dependent substitution, permutation and diffusion blocks. This makes the mechanism more secured. Also, we have enhanced the embedding capacity of the model by involving the Huffman compression mechanism which is lossless in nature. Hence, the data can be completely restored. Also, the LSB steganography technique involved in the proposed model is not only randomized in nature but also the embedding is done in the edges present in the cover image. This helps in the visual perceptibility of the data that cannot be seen by the human eye. Experimental results depict that the proposed model shows the best results in BER, UIQI, SSIM and visually as compared to other latest techniques available in the literature. Our model shows comparable results in terms of PSNR and MSE.

References

1. Cryptography and Network Security principles and practices. William Stallings, pearsons education, first Indian reprint 2003
2. Pooja KM, Kumar A (2010) Steganography—a data hiding technique. Int J Comput Appl 9(7). ISSN 0975-8887
3. Masud Karim SM, Rahman MS, Hossain MI (2011) A new approach for LSB based image steganography using secret key. In: Proceedings of 14th international conference on computer and information technology, pp 22–24
4. Gokul M, Umeshbabu R, Vasudevan, SK, Karthik D (2012) Hybrid steganography using visual cryptography and LSB encryption method. Int J Comput Appl 59(14):5–8
5. Gupta S, Goyal A, Bhushan B (2012) Information hiding using least significant bit steganography and cryptography. Int J Mod Educ Comput Sci 4(6):27
6. Mohammad AA, Abdel Fatah MA (2012) Public-key steganography based on matching method. Eur J Sci Res 223–231
7. Nivedhitha R, Meyyappan DT, Phil M (2012) Image security using steganography and cryptographic techniques. Int J Eng Trends Technol 3(3):366–371
8. Mathe R, Atukuri VRR (2012) Devireddy SK Securing information: cryptography and steganography. Int J Comput Sci Inf Technol 3(3):4251–4255
9. Islam MR, Siddiqa A, Uddin MP, Mandal AK, Hossain MD (2014) An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. In: Proceedings of 3rd international conference on informatics, electronics and vision, pp 1–6
10. Aung PP, Naing TM (2014) A novalsecure combination technique of steganography and cryptography. Int J Inf Technol Model Comput 2(1):55–62
11. Shingote Parshuram N, Hussain SA, Bhujbal PM (2014) Advanced security using cryptography and LSB matching steganography. Int J Comput Electron Res 3(2):52–55

12. Dhall S, Bhushan B, Gupta S (2016) An improved hybrid mechanism for secure data communication. Int J Comput Netw Inf Secur 8(6):67
13. Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A (2018) Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6:20596–20608
14. Tauhid A, Tasnim M, Noor SA, Faruqui N, Yousuf MA (2019) A secure image steganography using advanced encryption standard and discrete cosine transform. J Inf Secur 10(3):117–129
15. Akhshani A, Akhavan A, Lim SC, Hassan Z (2012) An image encryption scheme based on quantum logistic map. Commun Nonlinear Sci Numer Simul 17(12):4653–4661
16. Kumar R, Malik A, Singh S, Chand S (2016) A high capacity email based text steganography scheme using Huffman compression. In: 3rd international conference on signal processing and integrated networks (SPIN). IEEE, pp 53–56
17. Xuan L, Hong Z (2017) An improved canny edge detection algorithm. In: 8th IEEE international conference on softwareengineering and service science (ICSESS), pp 275–278. https://doi.org/10.1109/ICSESS.2017.8342913