Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.1, 2018, pp.93-98
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2018.7.1.1818

An Implementation of Text and Color Image Steganography Technique Using Cryptographic Algorithm

Prakhar Agrawal[1] and Arvind Upadhyay[2]
[1]PG Student, [2]Associate Professor, Department of Computer Science and Engineering,
Institute of Engineering and Science, Indore Professional Studies Academy, Indore, Madhya Pradesh, India
E-Mail: prakhar.agrawal277@gmail.com

(Received 23 February 2018; Revised 5 March 2018; Accepted 19 March 2018; Available online 27 March 2018)

Abstract - **The craft of data stowing away has gotten much consideration in the ongoing years as security of data has turned into a major worry in this web time. As sharing of delicate data by means of a typical correspondence channel have become inevitable, Steganography techniques aimed at secretly hiding data in a multimedia carrier such as text, audio, image or video, without raising any suspicion of alteration to its contents. The original carrier is referred to as the cover object. In this paper, we proposed a mechanism of end user data security by means of image steganography technique using ECDH (Elliptic Curve Diffie–Hellman) algorithm for improving image quality while we hide data in image. Our proposed approach is simplified yet efficient algorithm that can be implemented for end user application that strictly enforces the data integrity over the communication channel. The performance of the proposed approach is measured in terms of time, memory, MSE and PSNR which was better improved from the previous approach in the similar parameters.**

Keywords: **Steganography, Images, Cryptography, ECDH, RSA, Security, Data Hiding, Communication Channel**

I. INTRODUCTION

Now-a-day there is a rapid development of the Internet and telecommunication techniques. Importance of information security is increasing. Data security is a standout amongst the most difficult issues in the present innovative world. The extraordinary development of online applications in the World Wide Web requires the need to expand the security of information correspondences over the Internet, particularly for profoundly touchy archive exchange. Constantly communicated through the Internet are flows of information generated from many diverse applications such as e-commerce transactions, audio and video streaming or online chatting. The security of such data communication, which is required and vital for many applications nowadays, has been a major concern [1] [2].

An application such as secret communication, copyright protection, etc., increases the need for research of information hiding systems. Keeping in mind the end goal to anchor the transmission of mystery information over people in general system (Internet), different plans have been exhibited in the course of the most recent decade. Advanced pictures frequently have a lot of excess information and hence it is conceivable to shroud mystery message inside picture record. Images are the most common and widespread carrier medium for steganography. The general idea of hiding secret information in media has a wider range of applications that go beyond steganography [3].

Cryptography and Steganography are the real zones which take a shot at Information Hiding and Security. Steganography joined with cryptography, can be extraordinary compared to other decisions for taking care of this issue. Steganography is a computerized system for concealing mystery data into some type of media, for example, picture, sound or video. Steganography has developed into a routine with regards to hiding information in bigger record such that others can't associate the nearness with a concealed message. This system is by and large used to keep up the secrecy of profitable data to shield information from conceivable burglary or unapproved seeing [4].

II. BACKGROUND

Since the commencement of web the security of data is the most indispensable factor in data innovation and correspondence. Thusly, the foundation of an examination is an imperative piece of our exploration paper. It gives the unique circumstance and motivation behind the investigation. Subsequently there is requirement for foundation think about that adds to plan proposed framework.

A. Overview of Steganography

Since the start of web the security of information is the most pivotal factor in information development and correspondence. Various systems like cryptography, watermarking and encryption and unscrambling techniques were delivered remembering the ultimate objective to stay the information in the midst of correspondence. Unfortunately it was lacking to guarantee the substance of the puzzle message from outside phishers and developers. There was a need of another framework which can keep the nearness of the message puzzle. In the present data age, the progressions have developed so much that a substantial part of the customers slant toward web to trade data beginning with one end then onto the following over the world. So security in cutting edge correspondence is major essential when grouped information is being shared between two customers [5].

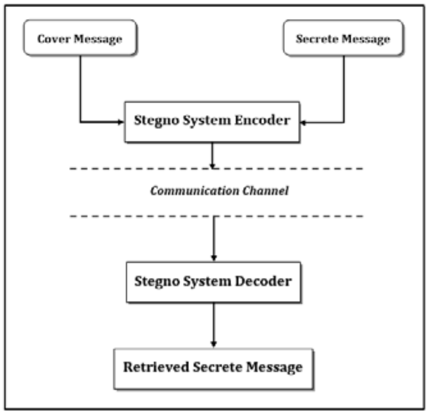

Fig. 1 Basic Steganographic System

Steganography is a procedure of concealing data. It disguises that the correspondence is occurring along these lines when utilizing steganography there is constantly mystery data is being transmitted and we attempt to make this data not to be found just by the planned recipient. The sender shrouds a message into a cover record likes for e.g. (picture, sound, video) and attempts to disguise the presence of that message, later the collector gets this cover document and identifies the mystery message and gets it [6].

Figure 1 demonstrates the steganographic framework. The protest which is utilized to conceal mystery data is called cover question. Stego message is alluded as a message that is acquired by implanting mystery message into cover message. The shrouded data might be either plain content, or pictures and so forth [6].

B. Requirement of Steganography

The three most critical necessities that must be fulfilled for steganographic procedure are limit, security, and heartiness as in figure 2. The assessment of steganography procedure is finished with these three parameters and there must be tradeoffs between these parameters to have better steganographic strategy.

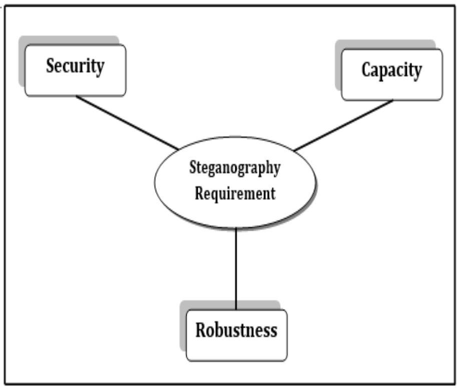

Fig. 2 Basic Requirements of a Steganographic System

1. Capacity

Capacity alludes to the measure of mystery data that can be inserted in the cover medium. Steganography goes for concealed correspondence and in this manner more often than not requires adequate installing limit. Steganographic limit is the greatest number of bits that can be inserted in a given cover document without influencing the nature of the cover medium and furthermore limiting the impression of the concealed information in the stego medium. The limit of the mystery message that will be inserted must be not as much as the extent of the cover medium [7].

2. Robustness

Robustness is the capacity to remove concealed data after normal picture handling tasks and the inserted information to stay flawless if the stego medium experiences stego assaults. The power prerequisite is required when exchanged with information concealing limit. In steganography heartiness is certainly not a best need, in this way steganographic frameworks are either not powerful against alterations or have constrained vigor against specialized adjustments [8].

3. Security

Security demonstrates a busybody's failure to identify inserted data. Such data can't be expelled past solid identification by focused assaults in view of a full information of the inserting calculation and the transporter with shrouded message. Keeping in mind the end goal to abstain from raising the doubts of assailants, the shrouded substance must be undetectable both perceptually and measurably. Hence, the qualities and characteristics of cover documents ought not be changed and no twists ought to be delivered amid the inserting procedure [9].

III. PROPOSED WORK

The aim of the work is to design and implement a technique which is highly secure and efficient for short messages exchange. In this section we included problem identification and methodology of data steganography technique

A. Problem Definition

Steganography turn out to be more essential as more individuals join the internet upset. Steganography turn out to be more essential as more individuals join the internet unrest. LSB is a standout amongst the most famous strategies which are utilized for concealing the mystery message. LSB concealing strategy fills in as it shrouds the mystery message straightforwardly at all two critical bits in the picture pixels, which influences the picture determination, because of this it decreases the picture quality and makes the picture simple to assault. In this manner there might be one plausibility to evacuate this issue and make the mystery message more secure and upgrade the nature of the picture is proposed.

The main problem area to be tackled in this work is the detection of attacker modification of a hidden secret message. The research work deals with the problem of enhancing the steganography performance by protecting any modification in the secret message by means of integrity verification that will help to identify possible modifications of a secret message that was not part of the original message.

B. Methodology

This section provides the detail methodology and basic functional aspects of the proposed image steganography approach and in the next section summarized steps of in algorithmic form.

C. Working Description

The working of the proposed image steganography technique is given and explained in details in this section. To understand the core concept of the proposed methodology by using given figure description

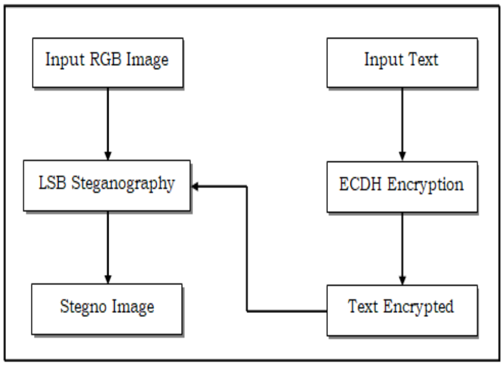

Fig. 3 Data Hiding Process

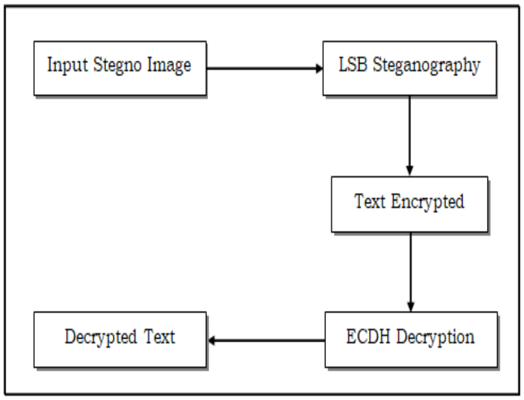

Fig. 4 Data Recovery Process

The given flow diagram 3 and 4 depicts image steganography process. Figure 3 show data hiding process (encryption) and 4 shows data recovery process (decryption). Here we are individually describing function flow of both diagrams. In above encryption process in figure 3, firstly we input an RGB based colour image and input text to be hide. After input image, parallel we input text which has to be hiding and secure using this image. Like an example, we take an input text "I am prakhar. My credit card number is 345677880025." This text to be hide into image after encryption. In the similar way, we apply encryption algorithm i.e. ECDH (Elliptical Curve Diffie–Hellman) on given input text. The encryption of the above given text

?Y???.`)?F+7;?b??/h?w??0???9f??WI{???Q?8???[?.??□
????????j?qL???-T?(?@??eI?5?~?6F~?`u???E??????a? z

For Image Steganography, we apply LSB based image Steganography technique on input RGB image. Therefore, text has been hided in image. Finally, the data have hidden using LSB Steganography successfully and produced new Stegno Image. Therefore, encryption process has been completed. Figure 4 depicts the data recovery process using decryption of data. Similarly, in this process, here we input generated Stegno image and apply LSB based stegamography on this image. After this process, we got cipher-text i.e. encrypted text. On this cipher-text, we apply ECDH algorithm for decrypting text data. Finally, decrypted text is produced from the image which is needed to be secure. This process also called data recovery process of original data. This over all process maintains the image quality and data security of end user. Hence, our approach for data security is much efficient and effective for data privacy and security applications.

D. Proposed Algorithm

The last segment gives the comprehension about the procedures associated with the proposed cryptographic based steganography strategy. This segment gives the abridged strides of the procedure for both the activity. This calculation is portrayed in table I and II.

TABLE I DATA ENCRYPTION (HIDE) PROCESS

Input: RGB Image (I_i), Text (T_i) Output: Stegno Image I_s
Process: 1. $I_i = \text{readInputImage}$ 2. $T_i = \text{inputText}$ 3. $\text{EncT} = \text{ECDH.encrypt}\ (T_i)$ 4. $\text{Stegno Image} = \text{LSBSteganography.hide}\ (I_i, \text{EncT})$ 5. Return I_s

TABLE II DATA DECRYPTION (RECOVER) PROCESS

Input: Stegno Image (I_s) Output: Original Text O_T
Process: 1. $I_s = \text{stegnoImage}$ 2. $\text{EncT} = \text{LSBSteganography.recover}\ (I_s)$ 3. $\text{DecT} = \text{ECDH.decrypt}\ (\text{EncT})$ 4. Return O_T

IV. RESULT ANALYSIS

The proposed image steganography technique is implemented successfully and for justifying the results and efficiency of the proposed technique. This section includes the results analysis and performance of the system in terms of their performance parameters.

A. Mean Square Error (MSE)

The mean squared error (MSE) of an estimator is one of numerous approaches to evaluate the contrast between values suggested by an estimator and the genuine estimations of the amount being assessed. MSE is a hazard work, comparing to the normal estimation of the squared blunder misfortune or quadratic misfortune.

In this figure 5 and table III, delineation of mean square blunder of information pictures for proposed and base strategy. The Mean Square Error is characterized as the square of the contrast between the pixel estimations of the first picture and the Stegno picture and afterward isolating it by size of the picture.

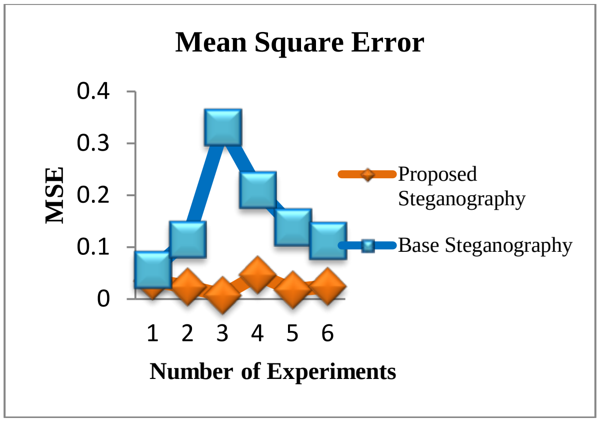

Fig. 5 Mean Square Error

The proposed image steganography technique show while X-axis depicts different experiment and Y-axis shows the error in percentages. The lower value of Mean Square Error (MSE) signifies lesser error in the Stegno image in other words better quality.

TABLE III MEAN SQUARE ERROR

No. of Experiments	Proposed Steganography A using ECDH	Base Steganography using RSA
1	0.0355	0.0561
2	0.0239	0.1153
3	0.0074	0.3312
4	0.0463	0.2100
5	0.0175	0.1386
6	0.0245	0.1124

B. PSNR (Peak Signal to Noise Ratio)

The PSNR measures the pinnacle motion to-commotion proportion between two pictures. This proportion is regularly utilized as quality estimation between the first and a packed picture. Higher the PSNR implies better the nature of the compacted or remade picture.

The PSNR value can be calculated as:

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right)$$

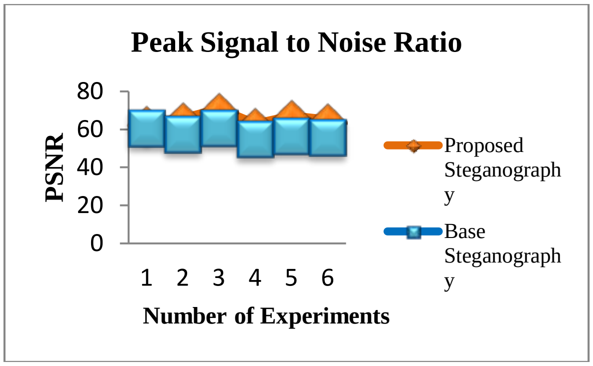

Fig. 6 PSNR

Peak signal to noise ratio of the proposed techniques for image steganographic is given using figure 6 and table III. In this diagram the X axis shows the different experiments and the Y pivot demonstrates the got PSNR proportion. The blue line demonstrates the base picture steganography procedure and Y-hub indicate proposed appproach. The measure of figured PSNR is fluctuating with the picture quality hence that isn't relies upon the picture estimate that is relies upon the nature of picture.

TABLE IV PSNR VALUES

No. of Experiments	Proposed Steganography A using ECDH	Base Steganography using RSA
1	62.62	60.63
2	64.33	57.51
3	69.40	60.87
4	61.46	54.90
5	65.69	56.71
6	63.77	55.82

C. Time Consumption

The amount of time required to process the selected proposed algorithm is known as time consumption. The evaluation of time usage is demonstrating using cryptography concept in figure 7 and table 4. In this chart the X pivot demonstrates the document measure (as far as KB-kilobytes) of pictures utilized for tests and the Y hub demonstrates the measure of time devoured for estimation of required time.

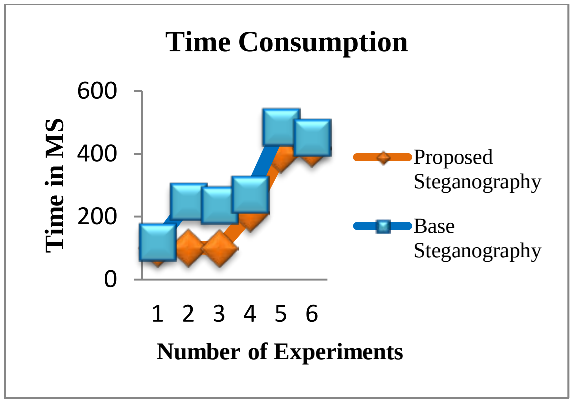

Fig. 7 Time Consumption

In this bar graph, we have plotted different experiments values for depiction of output variation. Blue line represents the base steganography approach for different experimental scenario, where green line shows the proposed approach of text hide. Moreover, with increasing size of data the time consumption of the proposed approach is increases. Therefore the proposed technique is more efficient and accurate for hiding data into image file a as compared to base RSA method.

TABLE V TIME CONSUMPTION

No. of Experiments	Proposed Steganography using ECDH	Base Steganography using RSA
1	101	119
2	102	248
3	100	238
4	212	271
5	401	485
6	419	452

D. Memory Consumption

The amount of main memory required to execute the implemented proposed algorithm is termed as space (memory) complexity or memory consumption.

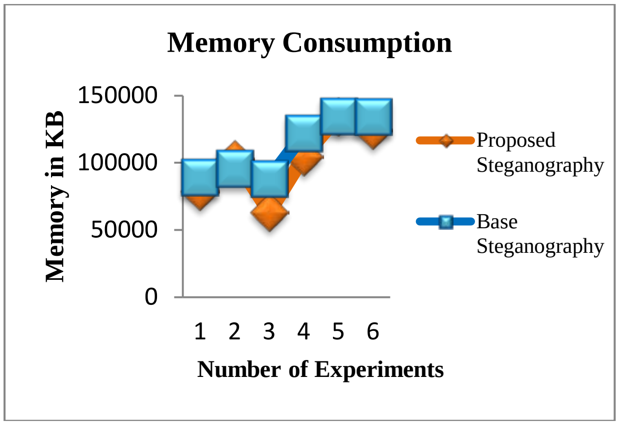

Fig. 8 Memory Consumption

The figure 8 and table VI shows the performance of the developed hide text in to image steganography algorithm. For results demonstration of both approaches the X axis shows performed experiments and the Y axis shows the memory consumption during encryption in terms of kilobytes. In order to show the performance of proposed and base algorithm in figure 8 where blue line is used for base steganography approach of hide text into image and green line show for proposed approach.

According to the given results most of the time the memory consumption is much stable for and many time it varies whenever we increases the image size. What's more of that the space multifaceted nature of the calculations is increments with the expanding size of exploratory pictures. Therefore the proposed algorithm is much adaptable due to constant memory consumption. For more clear performance we included tabular form of all output values in table VI.

TABLE VI MEMORY CONSUMPTION

No. of Experiments	Proposed Steganography using ECDH	Base Steganography using RSA
1	78898	89244
2	102543	95636
3	63208	88076
4	104712	121880
5	134488	134488
6	124585	134265

V. CONCLUSION AND FUTURE WORK

The main objective of the proposed LSB based steganography is to provide high degree of security during message exchange. Therefore a method is proposed and implemented. This section includes the conclusion of the work in this context additionally the future scope of the work is also included.

A. Conclusion

The development of present day correspondence needs exceptional methods for security particularly on PC arrange. As there shows up a hazard that the touchy data transmitted may be blocked or misshaped by unintended eyewitnesses for the transparency of the web. So it has brought about a dangerous development in secure correspondence and data covering up. In addition, the data concealing procedure can be utilized broadly in applications like business, military, advertisements, hostile to criminal, and computerized measurable et cetera.

In this security mechanism, the intention of the entire research work is to enhance security of user confidential data by proposing of image steganography technique. In this approach, we have proposed cryptographic based image steganographic technique which is based on pure encryption and decryption process by means of ECDH algorithm. The final outcome of the approach is used for network transmission or other task. Similarly the decryption operation required to recover the original data. On the basis of the analysis our approach is producing much better outcomes as compared base RSA based approach.

B. Future Work

The key aim of the proposed work for design and development of the efficient and secure cryptographic technique is accomplished successfully. In future the following possible work can be extending the application and performance of system.

1. In near future the proposed work is enhanced more for improving the cipher generation complexity enhancement to reduce the different kinds of attack effects.
2. It is also essential to enhance the system for improving the quality of image with increasing amount of data to be hiding.
3. The system can be test using more parameter of real world scenario.

REFERENCES

[1] A. Westfield and A. Pfitzmann, “Attacks on Steganographic Systems in Information Hiding”, *Springer-Verlag Heidelberg*, pp. 61-76, 1999.

[2] A. Abraham and M. Paprzycki, “Significance of Steganography on Data Security”, in *Proc. of the Information Technology: Coding and Computing, ITCC, IEEE,* Vol. 2, pp. 347-351, 2004.

[3] R. J. Anderson and F. A. P. Petitcolas, “On the Limits of Steganography”, *IEEE Journal on Selected Areas in Communications,* Vol. 16, No. 4, pp. 474-481, 1998.

[4] S. Gandharba and S. K. Lenka. “Classification of Image Steganography Techniques in Spatial Domain: A Study”, *International Journal of Computer Science & Engineering Technology,* Vol. 5, No. 3, pp. 219-232, 2014.

[5] K. Patel and S. Utareja, “Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm”, *International Journal of Computer Applications (IJCA),* Vol. 63, No. 13, 2013.

[6] G. R. Manjula and A. Danti, “A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain”, *International Journal of Security, Privacy and Trust Management (IJSPTM),* Vol. 4, No. 1, 2015.

[7] H. Wang and S. Wang, “Cyber warfare: Steganography vs. Steganalysis”, *Communications of the ACM,* Vol. 47, No.10, pp. 76-82, 2004.

[8] S. A. Laskar and K. Hemachandran, “An Analysis of Steganography and Steganalysis Techniques”, *Assam University Journal of Science and Technology,* Vol.9, No-2, pp. 88-103, 2012.

[9] S. Venkatraman, A. Abraham and M. Paprzycki, “Significance of Steganography on Data Security”, *Information Technology: Coding and Computing,* Vol. 2, pp. 347-351, 2004.