Devising an 'Image Steganography' Framework for an Enhanced Efficacy for Sequential Data Embedded System[1]

Ishaan Gupta
Bal Bharati Public School, Pitampura, New Delhi

DOI: 10.37648/ijrst.v10i04.004

Received: 10th August, 2020; Accepted: 21st September, 2020; Published: 25th October, 2020

ABSTRACT

The process of hiding information between images is called Steganography. The usage has been increased more in the current decade. Formed various methods and predictions to ad-lib the communication. It involves more with regards to the solid transmission of the information in the correspondence series. The data might be in any form like the text, picture, sound and even video records. Steganography all the more deeply utilizes the image as a medium to cover the first data. In the proposed strategy uses the adjusted type of Least Significant Bit (LSB) addition method. The first text record is first changed over into a parallel structure. The cover picture is changing over concerning the info information's comparing pixel game plan. The substitution happens so that one pixel worth will be altered and supplanted in each square. Therefore, the interloper can't discover the progressions that occurred inside the picture. This strategy utilizes the LSB procedure in a changed manner with pixel substitution. The trial results show that the proposed technique stays secure and is quick to process.

INTRODUCTION

A cryptographic computation with all conceivable keys and conventions is known as a cryptosystem. Every security framework should supply some security cycle that ensures the secret of the framework. A portion of the objectives that can be accomplished by cryptography is as follows: Authentication, Confidentiality, Access Control, Integrity, Non-renouncement, Availability and Accountability. In the cryptographic interaction, encryption and decryption demand a key. Some cryptosystems utilize a similar key together for encryption and decoding, called symmetric key or private key cryptography, and lopsided key or public-key cryptography might use unique keys together.

Steganography and Cryptography are two effective strategies to communicate confidential data safely. Advanced variation in correspondence has turned into an important piece of any framework that created numerous applications dependent on the Internet. It is required that the contact is made a secret. Steganography covers the first information inside the stego medium, which is as a picture. It conceals the info inside the image. Subsequently, it expresses that unapproved substances can't uncover the first data inserted inside the print.

Information stowed away covered picture is sent to the receiver side. An expected beneficiary can recover the confidential data utilizing an extraction computation and key that the sender gives. Steganography is the quality and study strategy used to send an individual message from a dispatcher to a beneficiary. A potential

[1] *How to cite the article:* Gupta I., Devising an 'Image Steganography' Framework for an Enhanced Efficacy for Sequential Data Embedded System, IJRST, Oct-Dec 2020, Vol 10, Issue 4, 30-37, DOI: http://doi.org/10.37648/ijrst.v10i04.004

hacker doesn't associate the resource with the private message. can do this by inserting the mysterious message inside another cover medium like the message, picture, sound or video. The word Steganography is of Greek beginning, and it characterizes hidden composing as" steganos signifying "covered or ensured" and realistic, signifying "stating" .

Steganography goes about as an answer that makes it conceivable to send data without dreading the messages being blocked and described. The drag of risky data is one more key utilization of Steganography. The paper is organized as follows. Area 2 involves related fields to the proposed procedure. Area 3 comprises the current strategies and the proposed approach to be executed. Area 4 contains the trial results and their degree. Segment 5 is trailed by the finish of the proposed method.

SUGGESTED WORK AND TECHNIQUE

Today it has transformed into a way to communicate natural mixed media data utilizing the unavoidable Internet. Using the inevitable electronic exchange, it has been incredibly fundamental to deal with the sensitive issue of bearing data security, especially in the present-day generation's. This part momentarily examines the different steganographic strategies and procedures utilized, different calculations used to conceal the information, and the proposed approach with the test results.

STEGANOGRAPHY TYPES

Steganography utilizes various types of media as the cover object and the recovery of the stego object. Some of them are the text, Image record, Audio document, Video File and IP convention. The text record utilizes advanced documents that don't contain excess information, and Audio and Video Steganography are more complicated to use. By and large, Image Steganography is being used for concealing individual information, and it stays the most reliable way of moving the news over the correspondence organization.

Since the power of the picture changes by 1 or 0 after the interaction has occurred, this picture Steganography strategy can be utilized and applied to the bitmap record pictures and the JPEG pictures. In JPEG design documents, every pixel is coded using the Discrete Cosine Transformation work (DCT).

Methods of Steganography

In the Least Significant Bit Encoding, the inspecting procedure is trailed by the quantization techniques. Before changing over, we will adjust the computerized information to the successive two-fold arrangement. Human Perception doesn't perceive the Noise of the stage coding at the sound signs, and the stage coding Steganography utilizes this technique. This method encodes the secret message bits as stage shifts in the stage range of a computerized signal, accomplishing an indistinct encoding as far as Peak - signal-to-commotion proportion.

The following methodology of Steganography, which conceals the information in network datagram, is the convention strategy. The principle point of this original strategy is to make the stego object imperceptible by the organization watchers. The data is put in the IP header of the datagram. In this technique, information to be hidden is situated in the IP header of a TCP/IP datagram.

Least Significant Bit (LSB) Technique

LSB is one of the old style and proficient steganography techniques; likewise, it is a replacement strategy. The course of this technique is to cover media LSB pixel esteems are subbed. It is a basic way of concealing the restricted information inside the cover picture. LSB inclusion procedure changing in regards to the no. of pieces in the image.

For a 24-digit picture, I would change the Red, Green Blue parts of the image. In this fundamental methodology, individual information is implanted at all huge pieces of the cover picture, which isn't uncovered effectively by likely intruders.

Proposed Technique

Hiding Algorithm

Step 1: Read the text message that has to be embedded.

Step 2: Convert the given text message to the corresponding binary sequence.

Step 3: Choose the cover image in which the secret data to be hidden.

Step 4: Find the Red, Green, Blue components of the image along with the pixel arrangement.

Step 5: Find two LSBs of each Red, Green and Blue pixel from carrier image.

Step 6: Apply a function on the LSB of the carrier image to obtain the position in such a way that, in the first block the least two red pixel value is substituted with the first two bits of corresponding binary sequence.

Step 7: In the second block, the two bits of green pixel are replaced with next two bits of the original text message.

Step 8: Finally, the blue components of the next block are replaced with a sequence of binary value.

Step 9: Iterate the process to insert two bits sequentially with every RGB component until the final pixel is inserted.

Step 10: Transfer the stego image obtained as a result of the above steps over the transmission medium.

Retrieval Algorithm

Step 1: Retrieve a stego image as an input.

Step 2: Find two LSB bits of each Red Green Blue pixel from the input stego image individually for each block.

Step 3: Apply a reverse function on the LSB to obtain the position of LSB's with hidden data.

Step 4: With help of these obtained positions, recollect the bits in order of two bits respectively.

Step 5: Finally, the original information will be retrieved.

The proposed strategy is created with the most un-amazing Bit replacement method in a changed manner. The accompanying calculation unmistakably states how the installing will be occurring to make the message safer.

(IJRST) 2020, Vol. No. 10, Issue No. IV, Oct-Dec **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

INVESTIGATION OUTPUT

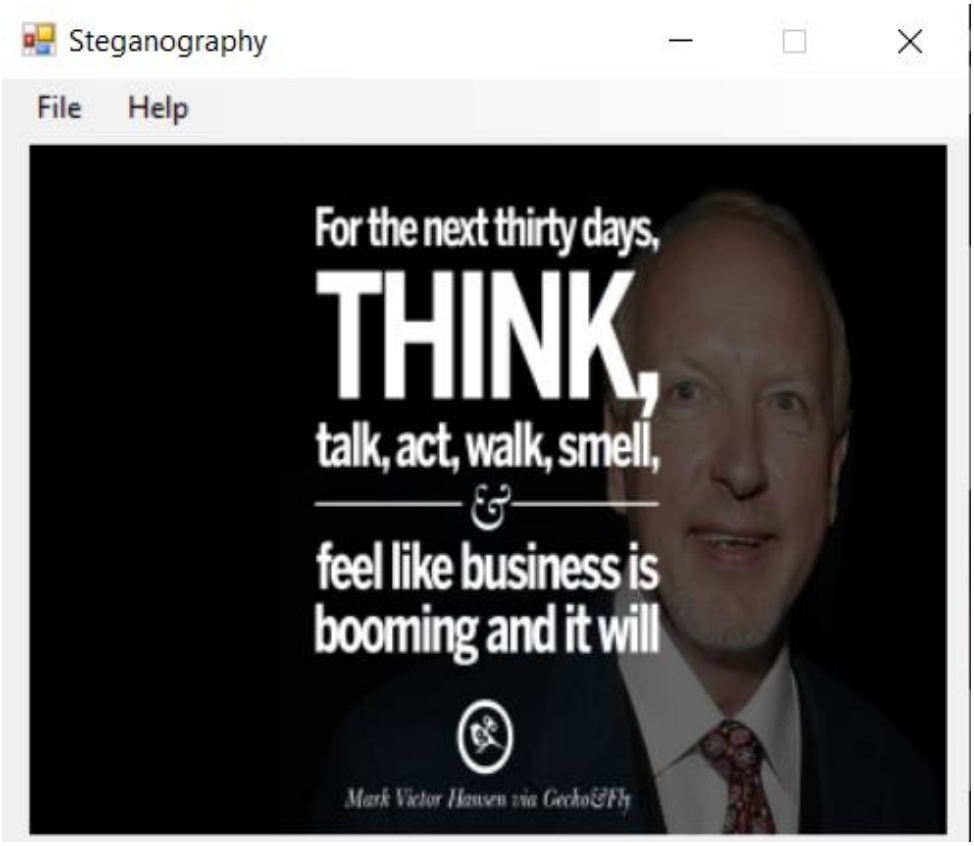

Fig 1: Process of Hiding Message

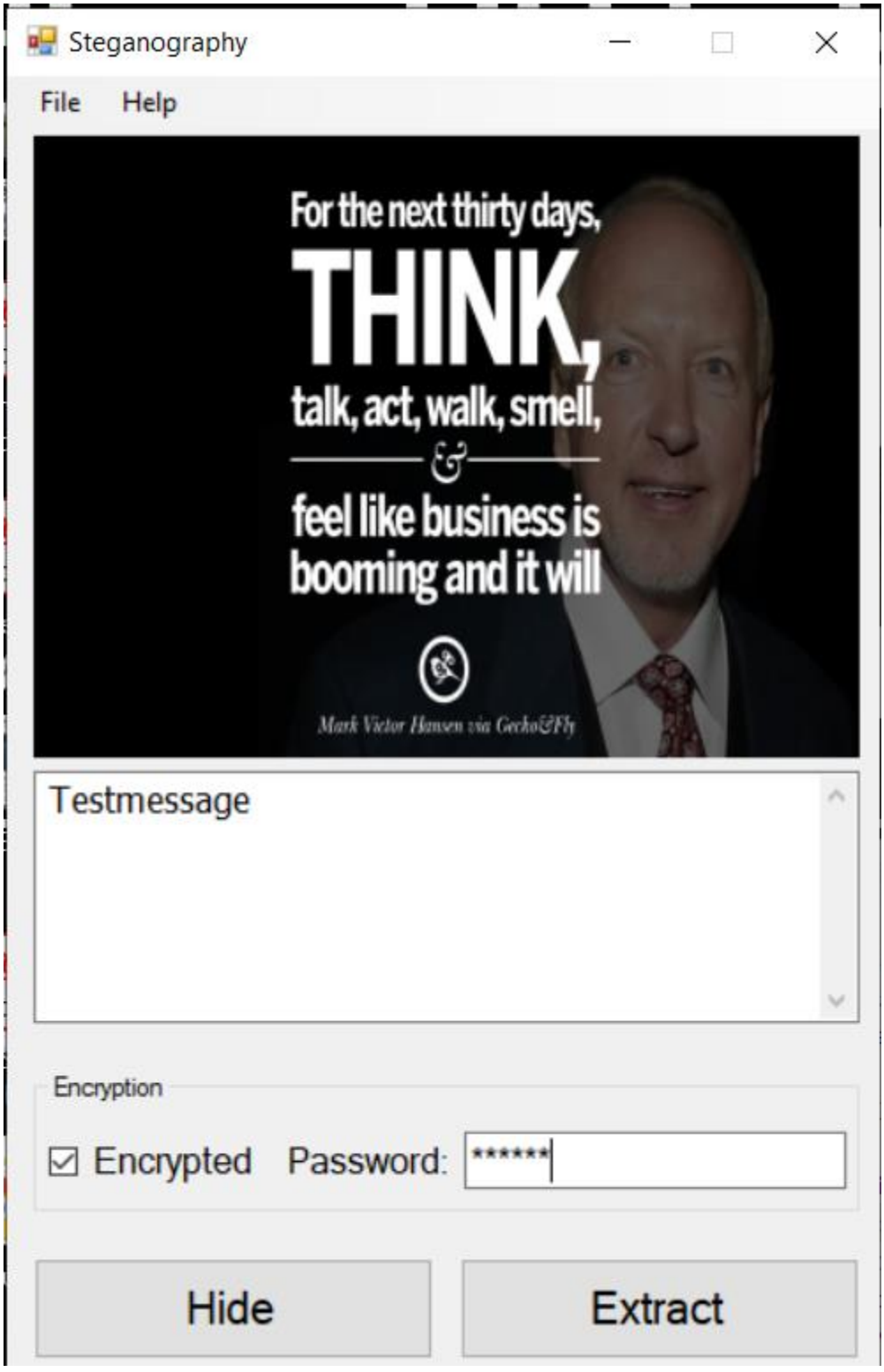

Fig 2: Process of Extracting Message

Our proposed approach has been approved by trying different things with varieties of pictures. The proposed framework has been executed in Visual Studio 2010, with .NET Framework Version 4.0 utilizing the C# windows application language.

In the above-demonstrated figures, figure (3) shows the information picture Baboon (a), Jet (c), and installed picture Baboon (b), Jet (d), shows the picture with the implanted text utilizing the proposed strategy.

Execution Evaluation

The presentation upsides of the PSNR determined from the yield picture is contrasted, and the PSNR esteems gave in the current procedures in the accompanying tables 1.

Input Image	LSB	DCT	DWT	Proposed Technique
Baboon	53.7558	58.3766	44.96	58.6673
Jet	52.7869	55.6473	44.76	53.9519

Table 1. Comparison of PSNR value between Existing method and proposed Technique

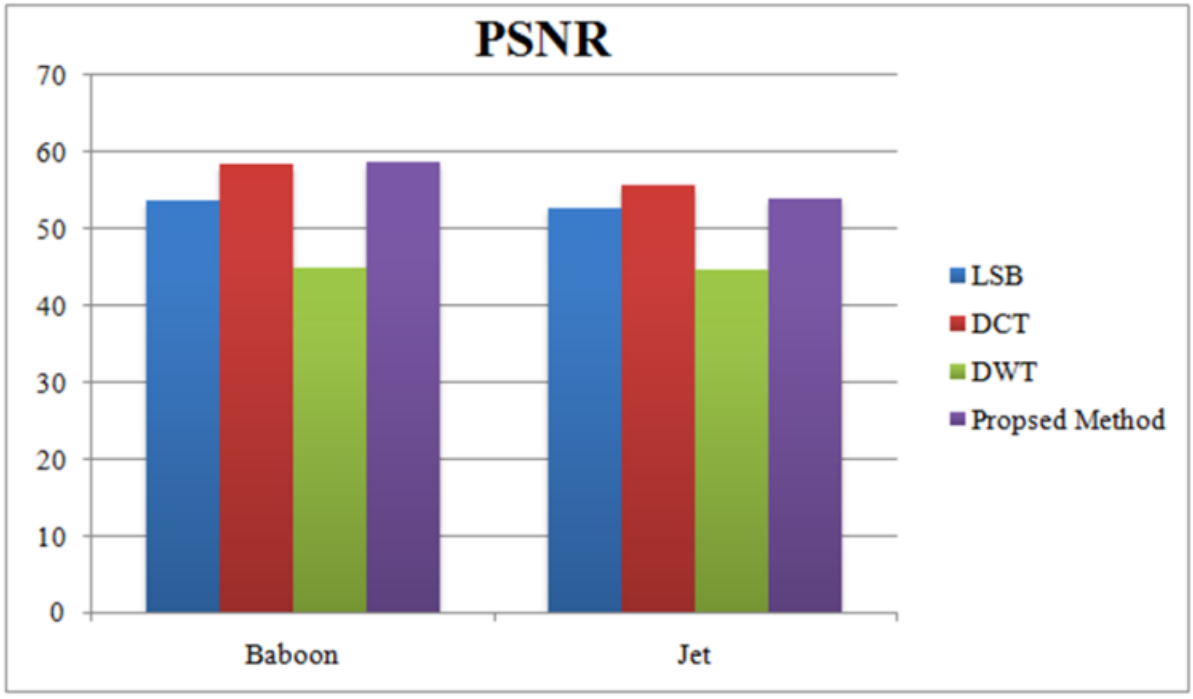

Chart 1 – PSNR Value of Baboon Image between existing and Proposed Technique

Comparative Analysis

The accompanying graph shows different execution measurements; for example, the pinnacle sign to clamour proportion was determined for the two info pictures and contrasted and the current strategy. It involves the LSB, DCT, DWT method and their close examination. This worth is contrasted and our proposed technique.

CONCLUSION

A Modified type of the LSB technique has been proposed and very much carried out to get the picture mystery. By the test results, we presume that no significant changes have been refined on the picture by utilising this proposed method, and it stays effective. By supplanting no less than a few pixels, less variety is made in the cover picture, which can't discover by human visual discernment. A predefined improved installed technique made it secure and quick to move

the data over any unstable channel or web. The exhibition of the created strategy has been broken down and contrasted on the straightforward LSB technique and the proposed technique in which acquired an awesome measurement and incentive for the stenographer picture.

REFERENCES

[1]. Ankit Chaudhary, J. Vasavada, J. L. Raheja, S. Kumar, M. Sharma, "A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images", in 22nd International Conference on Computer Graphics and Vision, 2012.

[2]. Bhavana.S, and K.L.Sudha, "Text Steganography Using Lsb Insertion Method Along With Chaos Theory".

[3]. Hemalatha S, U Dinesh Acharya, Renuka A, "Comparison Of Secure And High Capacity Color Image Steganography Techniques In Rgb And Ycbcr Domains", in International Journal of Advanced Information Technology (IJAIT) Vol. 3, No. 3, June 2013.

[4]. Shankar, K., and P. Eswaran. "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm", Artificial Intelligence and Evolutionary Computations in Engineering Systems. Springer India, 2016. 705-714.

[5]. Juan José Roque, Jesús María Minguet, "SLSB: Improving the Steganographic Algorithm LSB".

[6]. Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.

[7]. Mandal, J.K., Sengupta, M., (2011), "Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF).", Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298 – 301.

[8]. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key", International Conference on computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.

[9]. Mohammad A. Ahmad, Dr. Imad Alshaikhli, Sondos O. Alhussainan, "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No. 127-139, Sept., 2012.

[10]. Prabakaran Ganesan and R. Bhavani, "A High Secure And Robust Image Steganography Using Dual Wavelet And Blending Model", in International Journal of computer Science, Vol 9, Issue 3, pp:277-284.

[11]. Sachdeva, S and Kumar, A., (2012), "Color Image Steganography Based on Modified Quantization Table., Proceedings of Second International Conference on Advanced Computing & Communication Technologies , IEEE Conference Publications, pp 309 – 313.

[12]. Shilpa Gupta, Geeta Gujral, and Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography", in International Journal of Computational Engineering & Management, Vol. 15 Issue 4, pp:- 40- 42, July 2012

[13]. Soumyendu Das,Subhendu Das, Bijoy Bandyopadhyay, sugata sanyal, "Steganography and Steganalysis: Different Approaches".

[14]. Stuti Goel, Arun Rana, Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography", in IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48.

[15]. Shankar, K., and P. Eswaran. "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique", Journal of Circuits, Systems and Computers 25.11 (2016): 1650138.

[16]. József LENTI, "Steganographic Methods", in Periodica Polytechnica Ser. El. Eng. Vol. 44, No. 3–4, Pp. 249–258,2000.