ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 7, July 2015

A novel approach of Image steganography-hiding the confidential data into an image

Preeti Singh[1], Dinesh kumar Dhaka[2]

Student, Digital communication, RCEW, Jaipur, India[1]

Assistant Professor, Electronics and communication, RCEW, Jaipur, India[2]

Abstract: The paper proposed a new steganographyembedding and extraction system that uses Direct Sequence Spread Spectrum technique. DSSS is used to enhance the robustness and security of the system. Enhancement has been accomplished in strength on the cost of decreasing the capability of hiding. The noiselessness of the image steganography embedding and extracted is assessed by using peak signal-to-noise ratio (PSNR).

This steganography plan manages the extraction of the hide data without unique picture; consequently the visually impaired plan was acquired. Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR) are figured to measure picture quality. Likewise, the competency of the proposed technique is checked under normal picture preparing operations and a relative study is made against the previous technique .MATLAB R2012a has been used as an implementation platform.

Index Terms: Image steganography, Peak Signal to Noise Ratio (PSNR), Similarity Ratio (SR), Image quality.

I. INTRODUCTION

Steganography is the investigation of systems for concealing the presence of optional message in the vicinity of an essential message. Steganography is the craftsmanship and study of concealing the way that communication is occurring. The essential message is alluded to as the bearer sign or transporter message and the auxiliary message is alluded to as the payload sign or payload message. In data concealing, two unique variations of SS are for the most part utilized: recurrence bouncing and direct arrangement plans. The client typically perceived a lapse rate above which they got information is not reasonable. [1]

To secure the media content different advancements are utilized e.g. Cryptography, steganography and watermarking. Cryptographic methods are utilized to change the significance of the records. The approach of the Internet and the wide accessibility of PCs and printers make digital information trade and transmission a straightforward assignment. On the other hand, making digital information open to others through systems likewise makes opportunities for malignant gatherings to make marketable duplicates of copyrighted substance without consent of the substance proprietor [2]. Steganography strategies are utilized to hide the presence of the critical substance. Watermarking plans are utilized for security as well as authentication of mixed media content. [3]

A key is expected to insert messages into commotion. This key is utilized to produce pseudo-irregular key succession. We have a proposed a Random area choice to install the information inside of the spread sound. These varieties give a more secure framework, making speculations about the bit-rate or message length less feasible [4].

Steganography can be connected from multiple points of view to digital media. One technique for applying steganography is concealing data inside of pictures, for example, a photos or drawings. A typical strategy for concealing data in a picture is to store data bits inside of the slightest critical bits (or some other bit) of the pixels including the picture. Steganography can be utilized to shroud data inside of plain content records, sound, feature, and information transmission also. The security of Classical stenographic frameworks rely on upon keeping the encoding framework mystery, while cutting edge steganography tries to be imperceptible unless mystery data is known, to be specific, a mystery key. As a result of their obtrusive nature, stenographic frameworks leave discernible follows inside of a medium's attributes [4]. The steganography picture is made by supplanting the chose excess bits with the mystery message bits. One approach to keep the recognition of stenographic substance is to diminish the measure of the concealed message. Albeit such approach diminishes the probability of discovery, it is additionally brings about diminished concealing limit [5]. When all is said in done, the data concealing procedure comprises of the following steps:

1. Identification of repetitive bits in a spread medium. Excess bits are those bits that can be changed without corrupting the nature of the cover medium.
2. Selection of a subset of the excess bits to be supplanted with information from a mystery message. The steganography medium is made by supplanting the chose repetitive bits with the mystery message bits. Prior to the innovation of steganography and cryptography, it was trying to exchange secure data and, in this way, to accomplish secure communication environment. A portion of the strategies utilized in ahead of schedule days are composing with an undetectable ink, drawing a standard painting with some little adjustments, joining two pictures to make another picture, shaving the leader of the flag-bearer as a message, tattooing the message on the scalp and so on [6].

Secured development is required for associations. The period of encryption riddle keys with a lot of security is

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

IJIREEICE

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 7, July 2015

discriminating to ensure secure proceeding with data storage and is a trying purpose of examination. We need to improve our association. While building has changed the world association and preparing of developing countries are deficient. Adaptable keeping cash has getting typical in making and overpopulated countries, for instance, Bangladesh and India. This growing usage goes up against some security challenge. Trust and security issues of convenient sparing cash are similarly vital for making countries [7].

Rizky M. Nugrahaet. Al. [8] Image steganography has broadly creating. There are likewise various calculations creating for it. For the occasion, the consideration in utilizing sound information as insurance protest in steganography can be brought out late appearance than picture information. This examination ponders the execution of steganography in sound information utilizing Direct Sequence Spread Spectrum strategy. The Spread Spectrum system utilized as a part of this exploration is Direct Sequence Spread Spectrum. A key is obliged to insert messages into commotion, this key is utilized to deliver pseudo-clamor wave. The information to be inserted need initially balanced utilizing the pseudo-commotion.

Rami S. Youailet. Al. [9] recommended that Steganography is the science and craft of concealing that a communication is occurred. It inserts the classified record (sound or content or picture) in other transporter document. Content in picture steganography is measured in this work. The proposed steganography - framework uses Spread Spectrum strategy which is connected in lapse amendment coding together with spatial area. These are utilized to upgrade the heartiness and security of the framework. Discretionary position grouping inside of the spread picture pixels is likewise proposed in the work.

Ming Li et. Al. [10] states that the issue of removing visually impaired information that is installed more than a wide band in a range (change) area of an advanced medium (sound, picture and feature). This builds up a novel multicarrier mark iterative all around minimum squares (M-IGLS) center system to hunt down unidentified data covered up in hosts by means of multicarrier spread-range implanting. Neither the first host nor the inserting bearers are normal open. Exploratory studies on pictures demonstrate that the created calculation can achieve recuperation likelihood of slip near to what may be refined with host autocorrelation lattice and known inserting bearers. [11]

II. PROBLEM IDENTIFICATION

This is a period of imaginative communication and current advancements. With the advancement of digital and hand-held gadgets it is anything but difficult to make the digital substance. Sight and sound substance e.g. feature, voice, and pictures are additionally spared in digital structure. These substances are shared over online open group sites for different purposes with the goal of copyright insurance and approval. To secure the media content different methods are utilized e.g. cryptography, steganography, and watermarking. [12, 13]

- To actualize the steganography innovation through water checking's installing and extricating procedures.
- To enhance the security through picture encryption.
- Encrypting a message to create complete security.
- For finding possible path to enhance the image steganography encryption technology.

III. PROPOSED SOLUTIONS

A. Implementation Architecture

The system Design is defined as "The process of applying various techniques and principles for the purpose of defining a process or a system in sufficient detail to permit its physical realization". Various design features are followed to develop the system. The design specification describes the features of the system, the components or elements of the system and their appearance to end-users [14].

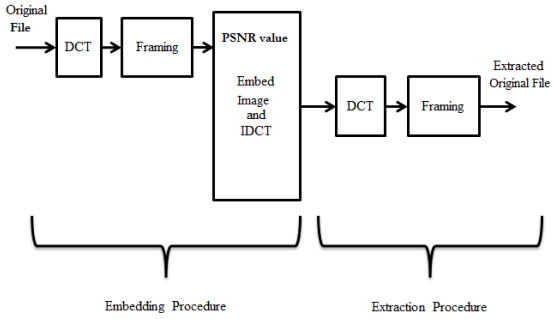

Fig. 1: System architecture of proposed solution [15]

The System architecture is shown by fig 1 for proposed algorithm. Conceptual design is known to be system architecture that outlines the behavior and structure of a system. System architecture is an organized description of any system that supports perceptive about the operational properties of that system [16]. It also describes the modules or building blocks of system and production plan to get desired results, and systems established, that will operate together to implement the complete system [17].

IV. RESULTS

The perceptible, imperceptible steganography and encryption is carried out to the picture for the security. Regardless of the fact that the sender breaks the encryption in the wake of accepting the picture from the owner, the perceptible and imperceptible steganography will secure the responsibility for specific picture from the sender [18]. The encryption is given for the data security from computer hackers and unapproved persons. In this manner the result will be the great security of the picture as shown by fig 4 to fig. 8. Fig 4 presents the sample file to be secured; and fig. 5 presents the embedding process of image and their authentication using steganography.

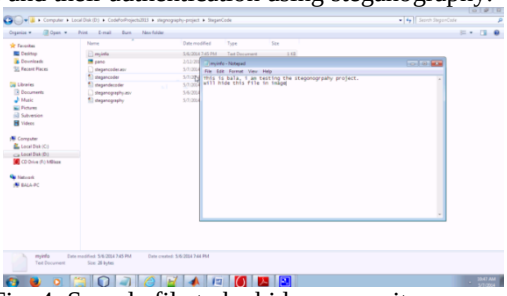

Fig. 4: Sample file to be hide as security purpose

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 7, July 2015

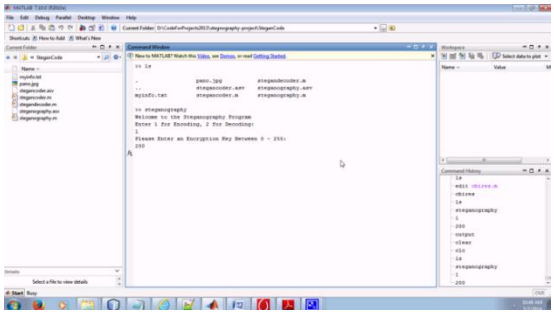

Fig. 5: Uploading the image file from which the text file is to be hiding

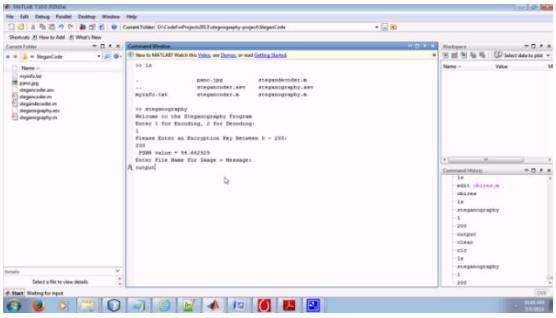

Fig. 6 The calculated PSNR value and encryption key for output values

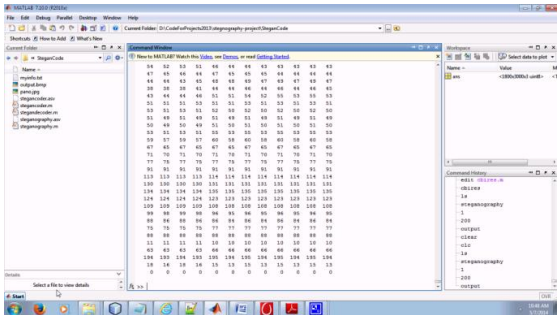

Fig. 7: Output values from range 0-255 as image graphic

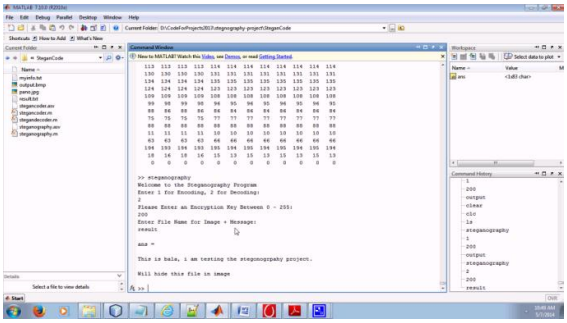

Fig. 8: Message of hiding file test into image

Fig. 6 presents the calculation of PSNR value for particular image to text file that induces in restoration process to original input images. As if we remove the steganography from output image this will return into original input images like as shown in below fig. 7 and 8 is restored with acknowledgment message. [19]

V. CONCLUSION

The paper initializes with discussion of the background of technologies used in literature study like steganography, cryptography and image encryption. Secondly the objectives of the research work. The system design and conceptualization mainly concentrates on few fundamental design concepts such as input & output design and system architecture. After that the main section i.e. proposed technique is with implementation procedure is explained with results. The simulation results show that the proposed steganography technique is better than the existing one.

VI. FUTURE WORK

In future, the security of strategy could be further upgraded by including more secure bit and byte control systems to the framework. Also likewise, installing the watermark with more security will be useful for the expanded protection. The results of PSNR, SSIM and MSE show that the noiselessness of our system is high and the technique is exceedingly robust.

ACKNOWLEDGEMENT

The authors convey their heartfelt thanks to **(Dr. Avinash Sharma)**, Principal, RCEW and **(Dinesh Kumar Dhaka)**, Director Cloud Computing Group, for providing them the required facilities to complete the project successfully. This paper is used to carry out a brief review about the image steganography techniques in security issues with authentication and encryption.

REFERENCES

[1] S.S.Sujatha, and M.MohamedSathik, “Feature Based Watermarking Algorithm by Adopting Arnold Transform”, Proc. of Springer International Conference on Information and Communication Technologies ICT 2010, Vol.1, pp.78-82, Sept 2010.

[2] C.Rey, and J.Dugelay, “A survey of watermarking algorithm for Image authentication”, Journal on Applied Signal Processing, Vol.6, pp.613-621, 2002.

[3] C.I.Podilchuk, and E.J.Delp, “Digital watermarking: algorithms and applications” IEEE Signal Processing Magazine, pp. 33-46, July 2001.

[4] ArvindkumarParthasarathy, and SubhashKak, “An Improved Method of Content Based Image Watermarking”, IEEE Transaction on broadcasting, Vol.53, no.2, pp.468 -479, June 2007.

[5] L.Xie, S.Wang, L.Gan, L.Zhang, and Z.Shu, “A class of authentication digital watermarks for secure multimedia communication IEEE Transactions on Image Processing, Vol.10, No.11, pp.1754-1764.

[6] M. Sonka, V. Hlavac. and R. Boyle, (1998) "Digital image processing," in: image Processing, Analysis, and Machine Vision, 2nd ed. http://www.pws.com

[7] D. Feldman, (2002) "A brief introduction to: information theory, excess entropy and computational mechanics," college of the Atlantic Sweden street, Bar Harbor, me 04609, http://hornacek.coa.edu/ computer society Press, 1998, pp. 381-386.

[8] Rizky M. Nugraha#1 Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data.In: 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia

[9] Rami S. Youail, Venus W. Samawi, Abdul- Karim A-R. In: Combining a Spread Spectrum Technique with Error-Correction Code to Design an Immune Stegosystem(2004)

[10] Ming Li, Michel K. Kulhandjian, Dimitris A. Pados, Stella N. Batalama, and Michael J. Medley, Extracting Spread-Spectrum Hidden Data from Digital Media, IN: IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013

[11] Ramana Reddy, MunagaV.N.Prasad, and D.SreenivasaRao, “Robust Digital Watermarking of Color Images under Noise Attacks”, International Journal of Recent Trends in Engineering, Vol.1, No. 1, May 2009.

[12] Q.Ying, and W.Ying, “A survey of wavelet-domain based digital image watermarking algorithm”, Computer Engineering and Applications, Vol.11, pp.46-49, 2004.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 7, July 2015

[13] Y.Wang, J.F.Doherty, and R.E.VanDyck, "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Trans. Image Process, 11, pp.77-88, 2002.
[14] S.H.Wang , and Y.P.Lin, "Wavelet Tree quantization for copyright protection for watermarking", IEEE Trans. Image Process, pp.154-165, 2002.
[15] P.Tao, and A.M.Eskicioglu, "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol.5601, pp.133-144, 2004.
[16] Y.Luo, L.Z.Cheng, B.Chen, and Y.Wu, "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp.1096-1103, 2005
[17] Yuan Yuan, Decai Huang, and Duanyang Liu, An Integer Wavelet Based Multiple Logo-watermarking Scheme. In IEEE, Vol.2 pp.175-179, 2006.
[18] H. Dobbertin, V. Rtjimen, A Sowa Ed., "Advanced encryption standard-AES," ser. Leture Notes in Computer Science/Security and Cryptography, Bonn, Germany: Springer, 2004, vol. 3373.
[19] Y.-Y. Chen, H.-K. Pan, and Y.-C. Tseng, "A Secure Data Hiding Scheme for Two-Color Images," in Proc. of 5th IEEE Symposium on Computers and Communications 2000, 2000, pp. 750-755.