iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Public Key Cryptography Based Reversible Data Hiding in Encrypted Images

Renuka[1], Revanasiddapa Kinagi[2], Vivekanand M Bonal[3]
[1]*Fourth Sem, M. Tech,* [2]*Asoc. Professor, Appa Institute of Engineering and Technology Karnataka,*
[3]*Head, R&D, Vivek InfoTehch, Kalaburagi, Karnataka India,*

Abstract: ***Now a day, more focus is on reversible data hiding (RDH) in encrypted images, so it maintains the excellent property that the original cover image can be easily recovered without any loss after embedded data. All previous techniques embed data by reversibly vacating room from the encrypted images, which may be leads to some errors on data extraction and image restoration. Also the hiding secret data in digital images, large varieties of techniques are available; some are more complex than others. Public key cryptography has various useful applications and the technique employed depends on the requirements of the application to be designed this technique suitable for medical and military applications***
Keywords: Image encryption, Lossless data hiding, Reversible data hiding, Public key encryption

I. INTRODUCTION

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption denies the message content to the interceptor. Usually encryption is used when one needs to keep his/her data private. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. Such an algorithm is necessary for the decryption of the message because without it, any party will be able to crack the code and access the data. Although for a well-designed encryption scheme, large computational resources and skill are required. An authorised recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorised interceptors.

The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. There are many transmission media to transfer the data to destination like e-mails; at the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are certain approaches like cryptography and steganography. Let us understand what cryptography and steganography means. Cryptography is the study of techniques for secure communication in the presence of third parties also called as adversaries.

More generally, it is about constructing and analyzing protocols that block these third parties with the help of various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography exists at the intersection of the rules and regulations of maths, computer science, image processing etc. There are many applications of cryptography which include computer passwords and e-commerce. Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier (in our case the Image) such that the changes so occurred in the carrier are not observable. Steganography is a useful tool that allows covert transmission of information over an over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval

II. LITERATURE SURVEY

A. *High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis AUTHORS N. A. Saleh, H. N. Boghdad.*

As of late information inserting over pictures has drawn huge enthusiasm, utilizing either lossy or lossless strategies. Albeit lossy procedures can permit extensive concealing limit, host picture can't be recouped with high constancy. A few applications require careful recuperation of the host picture, i.e. in drug understanding information can be implanted without influencing the restorative picture. By and large lossless information concealing procedures experience the ill effects of restricted limit as the host picture

ought to be kept in place. In this paper a lossless implanting strategy is proposed. In this method picture histograms are investigated to recognize the installing limit of diverse picture sorts. Histogram maxima and minima are utilized as a part of inserting limit estimation. The proposed method gives concealing limit that can reach up to half ofthe host picture size for pictures with expansive homochromatic districts (toons like).

B. Reversible Data Embedding Using a Difference Expansion AUTHORS:M. Bellare, S. Keelveedhi, and T. Ristenpart

Current distinction extension (DE) installing systems perform one layer implanting in a distinction picture. They don't swing to the following contrast picture for another layer inserting unless the present distinction picture has no expandable contrasts cleared out. The conspicuous burden of these procedures is that picture quality may have been extremely debased even before the later layer implanting starts on the grounds that the past layer installing has spent every single expandable contrast, incorporating those with extensive extent. In light of whole number Haar wavelet change, we propose another DE inserting calculation, which uses the flat and additionally vertical distinction pictures for information stowing away. We present a dynamical expandable distinction look and choice instrument. This system gives even opportunities to little contrasts in two distinction pictures and viably evades the circumstance that the biggest contrasts in the first contrast picture are spent while there is no opportunity to insert in little contrasts of the second distinction picture.

C. Reversible Data Hiding AUTHORS: Ni, Y.-Q. Shi

Advanced watermarking, frequently alluded to as information covering up, has as of late been proposed as a promising procedure for data confirmation. Inferable from information stowing away, be that as it may, some changeless bending may happen and subsequently the first cover medium will most likely be unable to be turned around precisely even after the concealed information have been removed out. Taking after the arrangement of information pressure calculations, this sort of information concealing calculations can be alluded to as lossy information stowing away. It can be demonstrated that a large portion of the information concealing calculations reported in the writing are lossy. Here, let us analyze three noteworthy classes of information concealing calculation. With the most prominently used spread-range water-stamping procedures, either in DCT area [1] or piece 8x8 DCT space [2], round-off blunder and/or truncation mistake might occur amid information implanting. Subsequently, there is no real way to turn around the stago-media back to the first without twisting.

D. Lossless Generalized-LSB Data Embedding AUTHORS: M. U. Celik, G. Sharma

We display a novel lossless (reversible) information installing method, which empowers the precise recuperation of the first host endless supply of the inserted data. A speculation of the understood slightest noteworthy piece(LSB) change is proposed as the information inserting strategy, which presents extra working focuses on the limit mutilation bend. Lossless recuperation of the first is accomplished by packing segments of the sign that are helpless to implanting mutilation and transmitting these compacted portrayals as a piece of the installed payload. A forecast based restrictive entropy coder which uses unaltered parts of the host signal as side-data enhances the pressure productivity and, in this manner, the lossless information installing limit.

E. Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding AUTHORS: X. Hu, W. Zhang, X. Li

Forecast mistake extension - based reversible information concealing plans comprise of two stages. Initial, a sharp expectation blunder histogram is produced by using pixel forecast methodologies. Second, mystery messages are reversibly implanted into the expectation blunders through growing and moving the PE histogram. Past PEE routines treat the two stages freely while they either concentrate on pixel expectation to get a sharp PE histogram, or go for histogram change to upgrade the implanting execution for a given PE histogram. This paper propose a pixel forecast technique taking into account the base rate measure for reversible information concealing, which builds up the consistency between the two stages basically. What's more, correspondingly, a novel improved histograms alteration plan is exhibited to surmise the ideal implanting execution on the produced PE arrangement. Analyses show that the proposed system beats the past condition of-craftsmanship partners essentially as far as both the forecast precision and the last installing execution.

III. MODULES AND MODULE DESCRIPTION

A. Modules

1) Input image initialization,

2) Image Encryption,

3) Data Embedding,
4) Data Extraction and Image Recovery,
5) Compute PSNR.

B. Module Description

1) Input Image Initialization: In this module, we initialize the given image (i.e.) get the input image from user by using the keyword 'uigetfile'. This contains only the pathname and filename. To read the image filename, we used 'imread' command. This read image was store in a variable as a matrix. Then we estimate the size of the given image using 'size' command. This give information of size of given image to estimate whether the given text was within the size of input image

2) Image Encryption: Assume the original image with a size of N1XN2 is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as $b_{i,j,0}, b_{i,j,1}, \ldots, b_{i,j,7}$ where 1<=i<=N1 and1<=j<=N2, the gray value as, and the number of pixels as N(N=N1XN2). That implies $b_{i,j,u} = [p_{i,j}/2^u] \bmod 2$, u=0,1,2,…,7 In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated.

3) Data Embedding: In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters. The detailed procedure is as follows. According to a data-hiding key, the data-hider pseudo-randomly selects N_p encrypted pixels that will be used to carry the parameters for data hiding

4) Data Extraction and Image Recovery: In this phase, we will consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. With an encrypted image containing embedded data, if the receiver has only the data-hiding key, he may first obtain the values of the parameters and from the LSB of the selected encrypted pixels. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content

5) Compute PSNR Value: In this module we compute the PSNR value for input image and decrypted image. Peak Signal-to-Noise Ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.PSNR is most easily defined via the mean squared error (*MSE*). Given a noise-free *m*×*n* monochrome image *I* and its noisy approximation *K*, *MSE* is defined as:

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

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

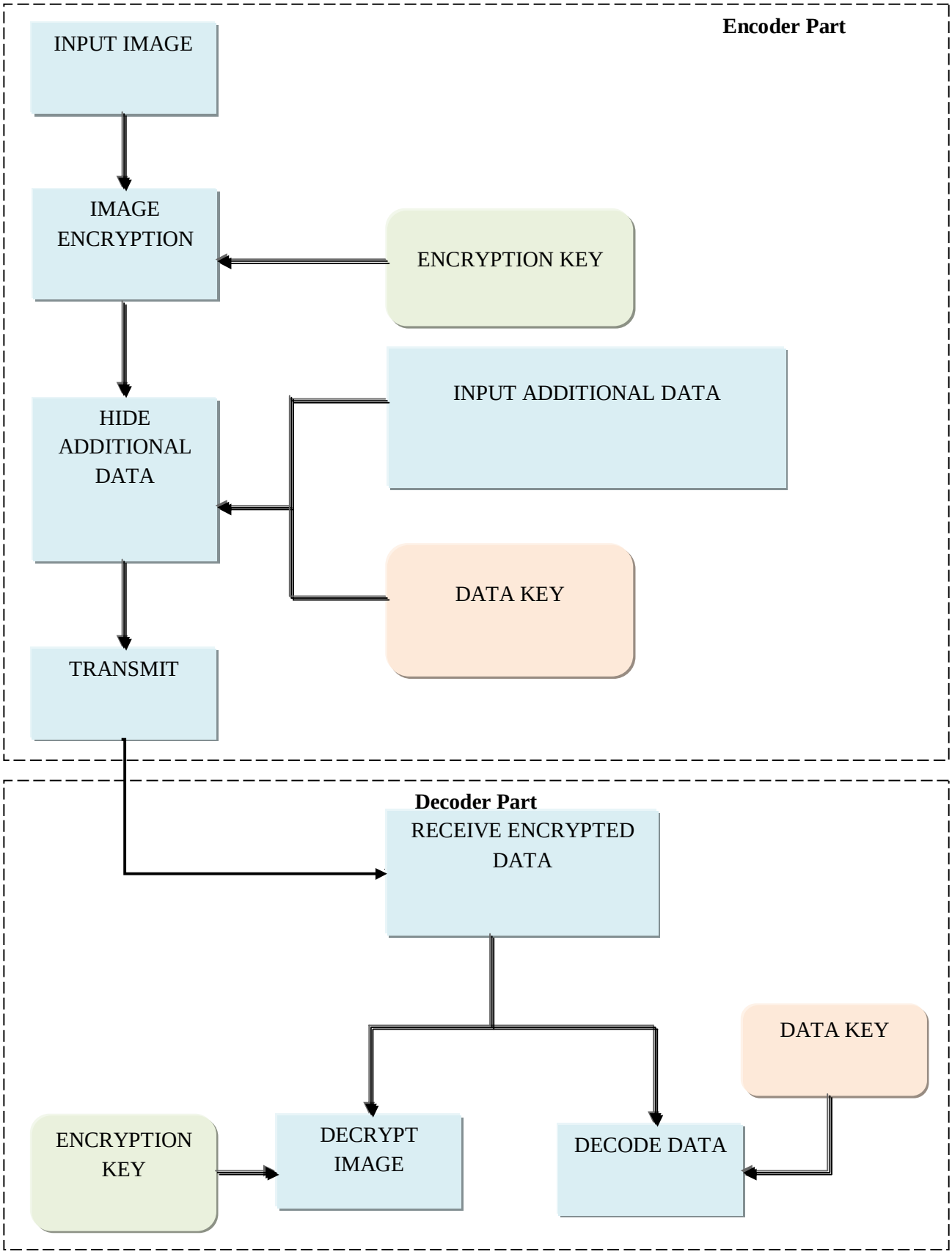
$$= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right)$$

$$= 20 \cdot \log_{10} (MAX_I) - 10 \cdot \log_{10} (MSE)$$

Using this PSNR value we can compare our algorithm with other algorithm that our method gives better result than previous method.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

IV SYSTEM ARCHITECTURE



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

IV. IMPLEMENTATION RESULTS

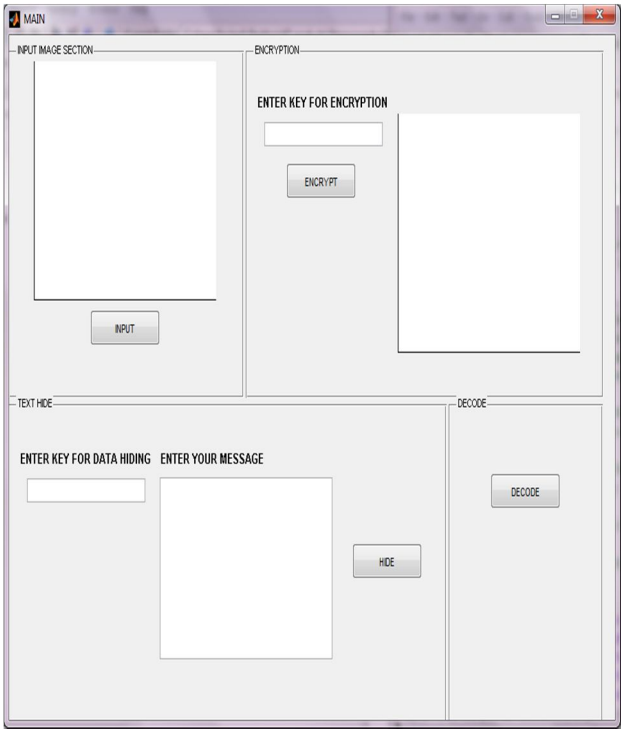
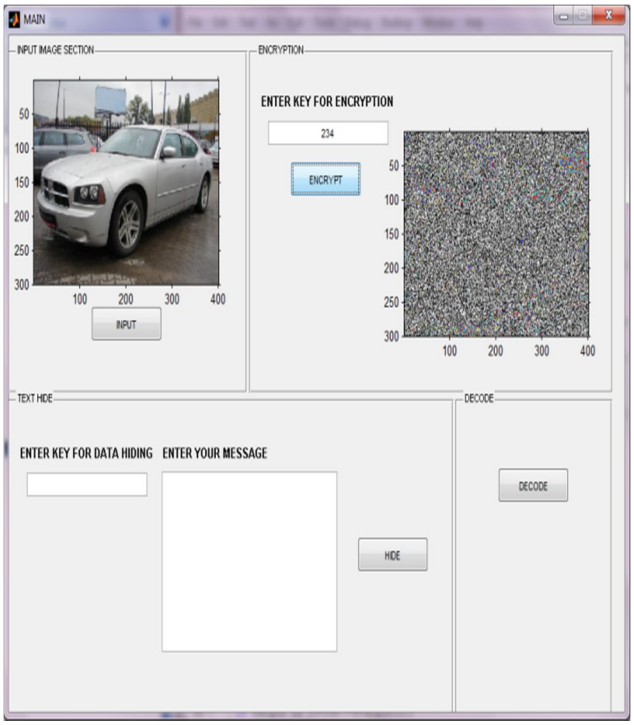
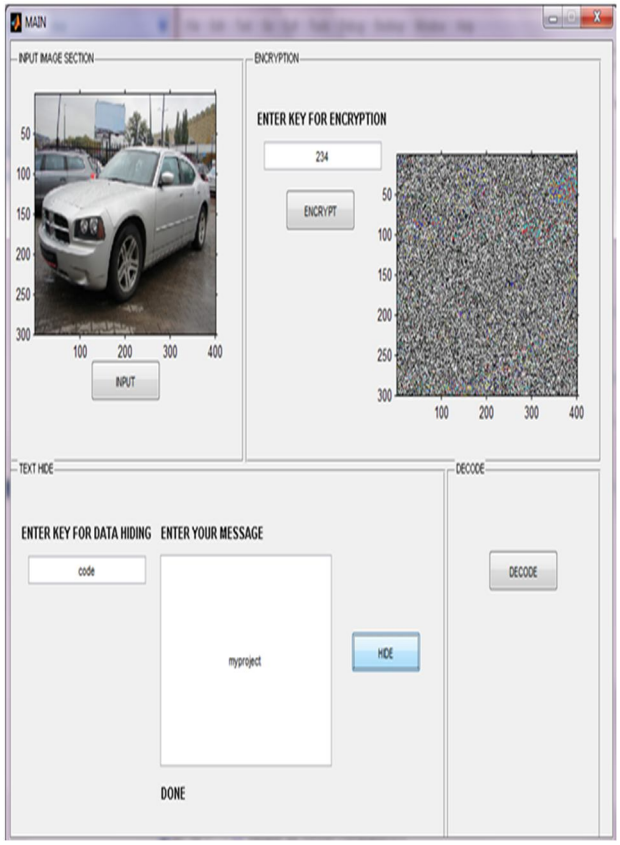


Figure 4 Data with Key



Figures 5 Selecting Image for Decode



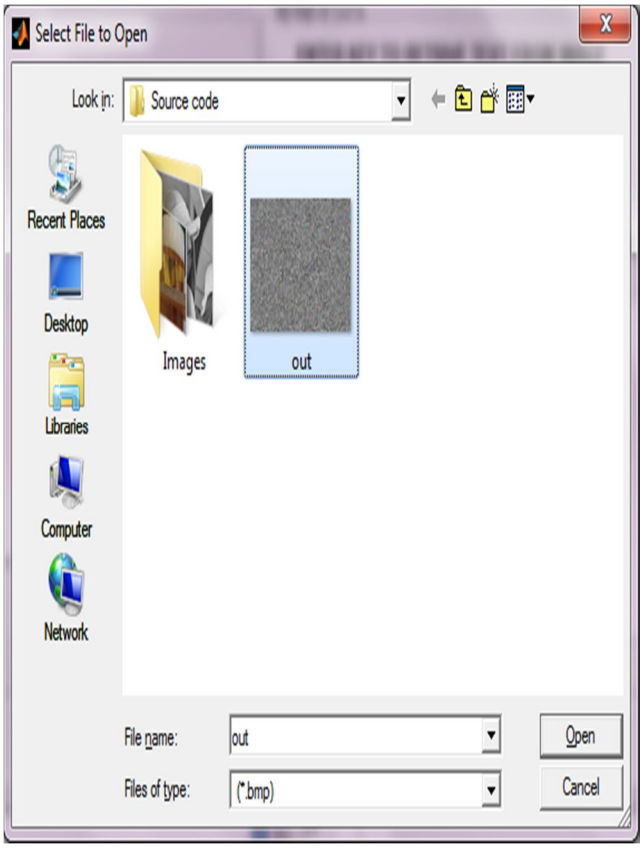


Figure 6 Entering Wrong Code

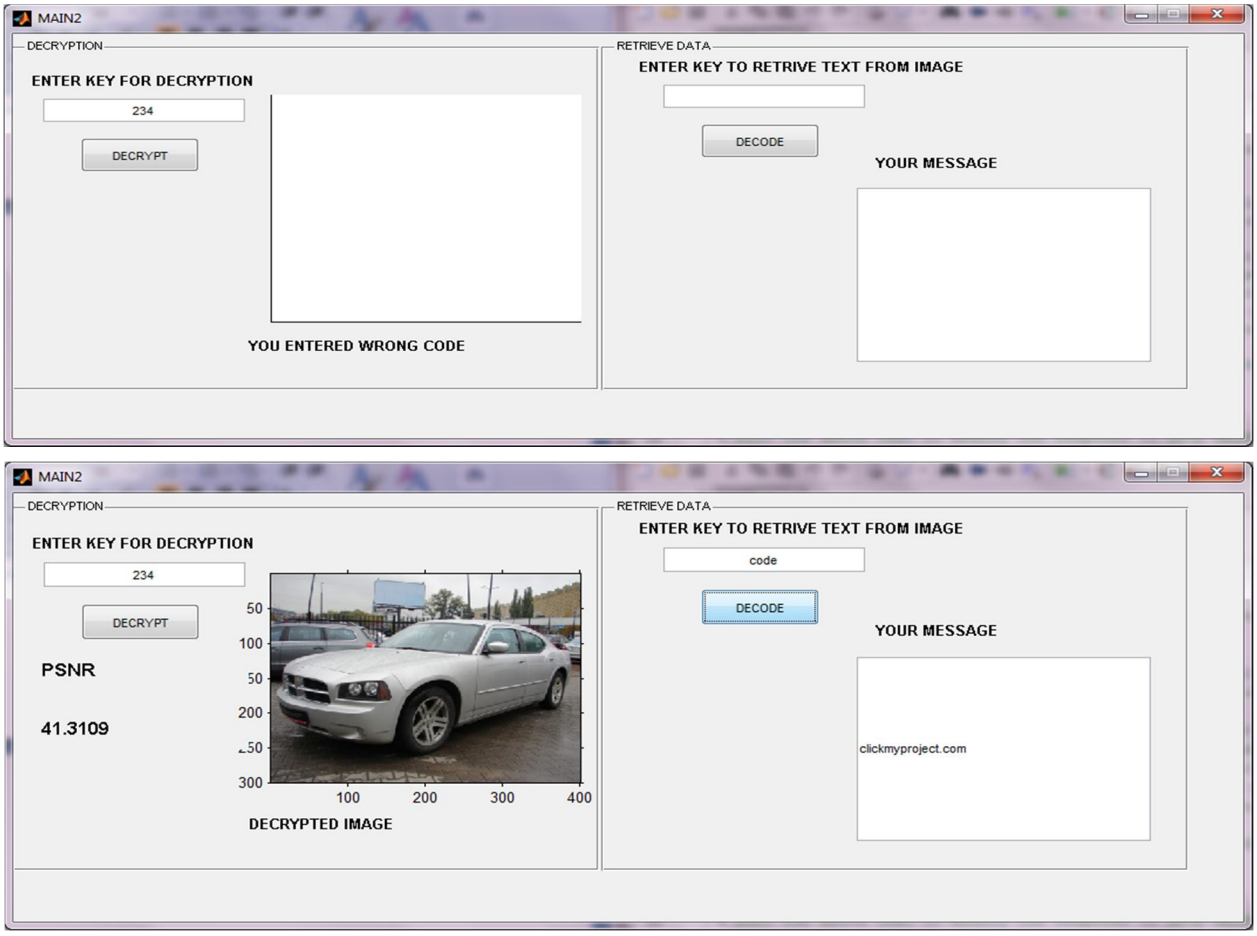


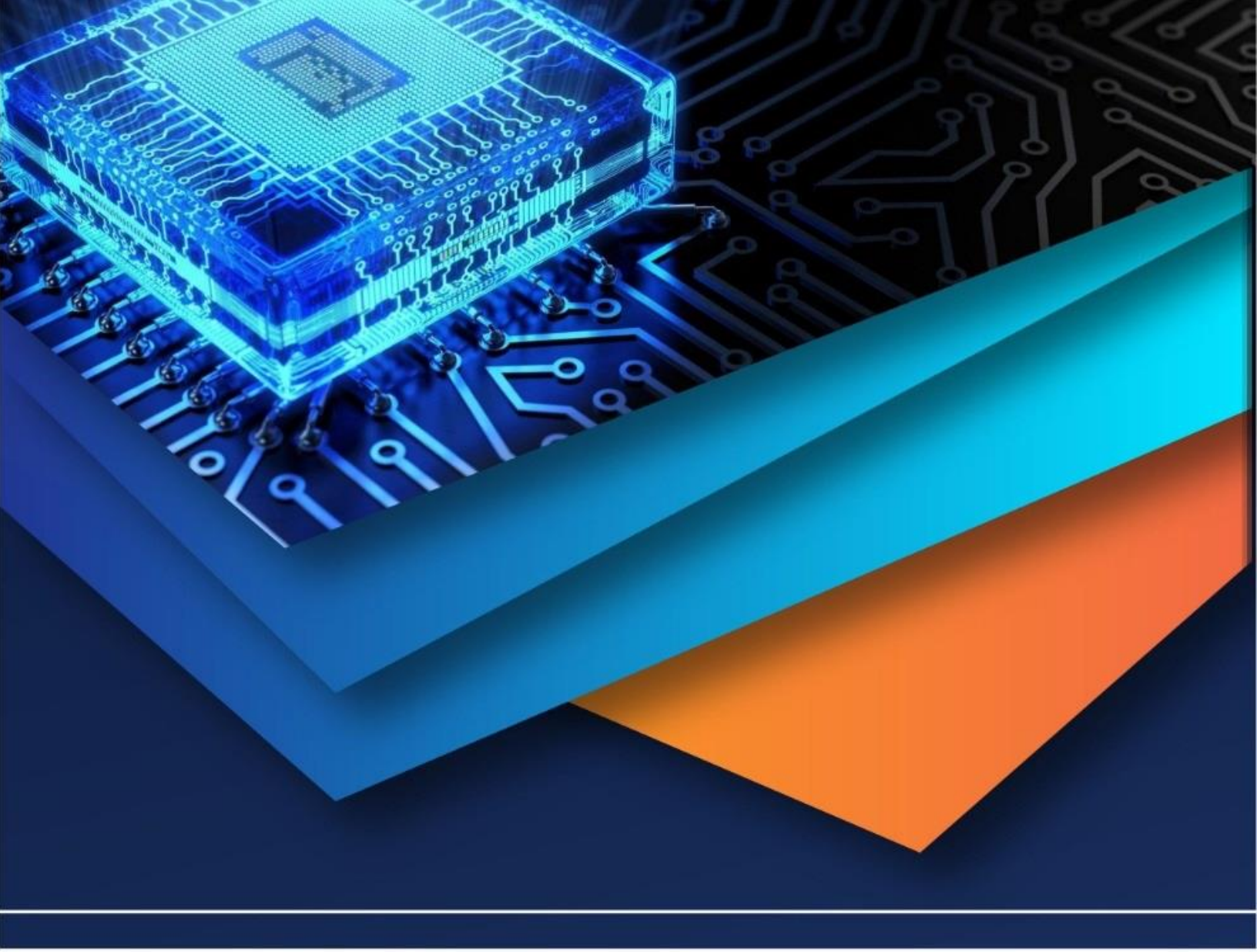
Figure 6 Entering Correct Code

V. CONCLUSION

In this paper, a reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key by using Hill-chipher method. Here we include another key act as password to decrypt the encrypted image. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

REFERENCES

[1]. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.
[2]. X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011
[3]. W. Liu, W. Zeng, L. Dong, and Q. Yao,"Efficient compression of encrypted grayscale images,"IEEETrans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[4]. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.
[5]. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180– 187, Feb. 2010.
[6]. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[7]. M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," IEEE Trans. Image Process., vol. 14, no. 12, pp. 2129–2139, Dec. 2005.
[8]. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY