International Journal of Engineering and Techniques - Volume 3 Issue 3, May-June 2017

RESEARCH ARTICLE OPEN ACCESS

# A New Data Hiding Technique Using CHAOS Embedded for Colour Image

N Mallikarjuna[1] , P.Varunraj[2] , K.Santhosh Kumar[3]

ECE Department,SRM University, Chennai

## Abstract:

Data hiding algorithms, which have many methods describing in the literature, are widely used in information security. In data hiding applications, optimization techniques are utilized in order to improve the success of algorithms. The genetic algorithm is one of the largely using heuristic optimization techniques in these applications. Long running time is a disadvantage of the genetic algorithm. In this paper, chaotic maps are used to improve the data hiding technique based on the genetic algorithm. Peak signal to noise ratio (PSNR) is chosen as the fitness function. Different sized secret data are embedded into the cover object using random function of MATLAB and chaotic maps. Randomness of genetic is performed by using different chaotic maps. The success of the proposed method is presented with comparative results. It is observed that gauss, logistic and tent maps are faster than random function for proposed data hiding method.

## I. Introduction

The term digital image refers to processing of a two dimensional picture by a digital computer. In a broader context, it implies digital processing of any two dimensional data. A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25

frames per second to produce a visually continuous display.

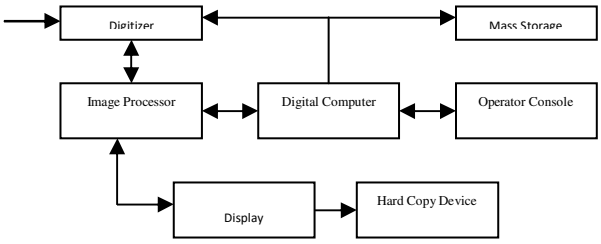



FIG 1.1 BLOCK DIAGRAM FOR IMAGE

### *1.1.1 THE IMAGE PROCESSING SYSTEM*

*DIGITIZER:*

A digitizer converts an image into a numerical representation suitable for input into a digital computer. Some common digitizers are

1. Microdensitometer
2. Flying spot scanner
3. Image dissector
4. Videocon camera
5. Photosensitive solid- state arrays.

*IMAGE PROCESSOR:*

An image processor does the functions of image acquisition, storage, preprocessing, segmentation, representation, recognition and interpretation and finally displays or records the resulting image. The following block diagram gives the fundamental sequence involved in an image processing system

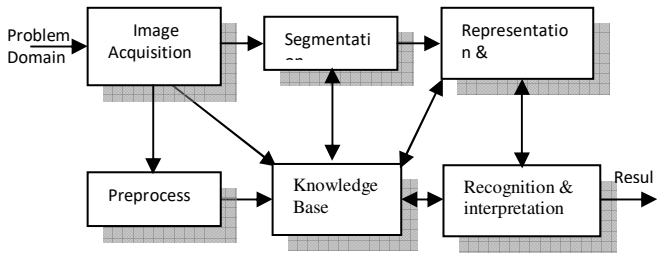



*FIG 1.2 BLOCK DIAGRAM OF FUNDAMENTAL SEQUENCE INVOLVED IN AN IMAGE PROCESs*

As detailed in the diagram, the first step in the process is image acquisition by an imaging sensor in conjunction with a digitizer to digitize the image. The next step is the preprocessing step where the image is improved being fed as an input to the other processes. Preprocessing typically deals with enhancing, removing noise, isolating regions, etc. Segmentation partitions an image into its constituent parts or objects. The output of segmentation is usually raw pixel data, which consists of either the boundary of the region or the pixels in the region themselves. Representation is the process of transforming the raw pixel data into a form useful for subsequent processing by the computer. Description deals with extracting features that are basic in differentiating one class of objects from another. Recognition assigns a label to an object based on the information provided by its descriptors. Interpretation involves assigning meaning to an ensemble of recognized objects. The knowledge about a problem domain is incorporated into the knowledge base. The knowledge base guides the operation of each processing module and also controls the interaction between the modules. Not all modules need be necessarily present for a specific function. The composition of the image processing system depends on its application. The frame rate of the image processor is normally around 25 frames per second.

**1.2** BJECTIVE AND SCOPE OF THE PROJECT

Optimization techniques are used to solve some complex problems. There are some limitations to the optimization techniques used in solving complex problems. In this paper, the data hiding problem is optimized using genetic algorithm. In the genetic algorithm steps, single point crossover operator is applied and themutation point is randomly selected. PSNR, which is a visual quality metric, is used as fitness function. Row, column and layer information of image are used for generating the population. For 512 × 512 × 3 sized image, individuals consist of 20 bits (_log2512 × 512 × 3_ bits). The genetic algorithm is used to embed secret data into the best indices. Random function of MATLAB and chaotic maps are applied for testing the randomness of the genetic algorithm.

**1.3** EXISTING SYSTEM

The idea of secretly sending information has seen its importance as old as the communication evolved itself. Steganography is nothing but to embed the secret information in an image, audio or in a video. The sensitive image that contains the secret information is called the stego-image. This information hiding makes sure that only the sender and receiver can suspect the existence of secret information in the image. The main advantage of the steganographic technique is that the secret information does not draw attention (remains subtle). In this way the hidden information is highly secured. Shannon-FanoElias is one technique of embedding the secret information where the embedding of secret string is done by generating a code word for each character in a string. By this technique high degree of data encryption is made possible. In order to make sure that the stego images are not being easily intruded, a check of the quality of stego images is done by calculating the Peak Signal To Noise Ratio (PSNR) and Mean Square Error (MSE). This paper provides a simple avant-garde review and the various analysis of the Shannon-Fano-Elias algorithm with some standards and general rules unfolded from various analysis..

1.3.1 DISADVANTAGES OF EXISTING SYSTEM

- Low PSNR
- High computation time

1.4PROPOSEDSYSTEM

Optimization techniques are used to solve some complex problems. There are some limitations to the optimization techniques used in solving complex problems. In this paper,

the data hiding problem is optimized using genetic algorithm. In the genetic algorithm steps, single

point crossover operator is applied and themutation point is randomly selected. PSNR, which

is a visual quality metric, is used as fitness function (Zhang et al. 2014). Row, column and layer information of image are used for generating the population. For 512 × 512 × 3 sized image, individuals consist of 20 bits ($\log_2 512 \times 512 \times 3$ bits). The genetic algorithm is used to embed secret data into the best indices.

BLOCK DIAGRAM


1.4.2 PROPOSED SYSTEM ADVANTAGES

- The proposed data hiding algorithm hide data without loss of image quality
- Provide suitable solution with high PSNR

PROJECT DESCRIPTION

2.1 INTRODUCTION

- Nowadays, providing information security has become one of the most important subjects in parallel with improving internet technology. The leading information security techniques are data hiding, watermarking and cryptography . Data hiding techniques are widely used in information security. The goal of data hiding techniques is to embed the secret message into a cover object without making any perceptual changes . The object including the hidden message is usually named as the stego-object. Stego-objects' visual quality must be high because there must be little difference between the stego-object and the original cover object . A good data hiding technique should include high payload capacity, robustness and high visual quality. In recent years, the chaos concept has attracted researchers' attention. The chaotic systems are applied to generate
- random pixels in data hiding because chaos-based algorithms have higher security and complexity than the classical data hiding algorithm .

**2.2DATA HIDING IN IMAGES:**

- The popular saying 'a picture is worth a thousand words' was certainly true until last decade but, the growing research interests in the field of digital image processing during the last decade have changed this estimation about a picture. Now pictures in their digital representations speak much more than a thousand words, thanks to the digital image data hiding procedures. Steganography in which we generally embed some secret message into an innocuous looking simple image(called as the cover image) and create a Stego image. The Stego image visually seems to be indifferent from the original cover but hides the secret message inside it and is transmitted to the desired recipients over the communication channels without creating any suspicion in the minds of the intermediately sniffers or/and receivers. When the authorised recipient receives the image, they follow the extraction procedure to retrieve thesecret message. To increase

the secrecy or security of the hidden message there may some keys involved in this

- process of embedding and extraction. At the transmission end, during embedding, the message can suitably be encrypted using one or more encryption techniques. These encryption standards can be key based encryptions or non-key based and in key based techniques, they again can be public or private or a mix. Depending upon the encryption method used during the embedding process, the receiver needs to execute certain decryption algorithms to retrieve the correct message. If any of the decryption algorithms or the keys used for the procedure or the sequence is not known to the receiver then the extraction fails and the receiver cannot retrieve the message

- Information hiding techniques are broadly classified into four categories such as, Covert channels, Steganography, Anonymity and Copyright marking . The Steganographic procedures can be linguistic or technical whereas the copyright marking procedures can be robust or fragile. Watermarking is a type of robust copyright marking technique which can further be classified as perceptible or imperceptible watermarking. A covert channel is a type of computer security attack [6] that provides a channel for transfer of information in a way that violates the computer security policy. Robustness and imperceptibility are the important characteristics of a covert channel. Linguistic Steganography (Text Steganography or Cryptography) uses text as the cover media to hide the secret message

- whereas the technical covert channels work by exploiting the loopholes in the OS, network model, protocols etc. Copyright marking is a procedure that is used to protect the intellectual properties. In this method a logo or a mark is embedded into a piece of information to show the originality of the work. The copyright can be robust or fragile depending upon the requirement. Fragile copyright marks are used to prove manipulations as the fragile marks cannot resist manipulations and lost upon slightest modifications. Robust copyright methods are resistant against all sorts of statistical and other types of manipulations. Finger printing and watermarking techniques [9] are popular types of robust copyright marking methods and are used for authentication purposes [10]. Table 2 compares watermarking against Steganography. Figure.6 shows the experimental results of spatial domain visible watermarking in which a 32X32 pixel monochrome watermark is embedded into the higher order bit plane of the 256X256 pixel gray scale Woman image and then the watermark is retrieved after the watermarked image is subjected to various types of statistical attacks such as format change, resizing, compression, rotation etc. , a 20x20 pixel gray scale watermark is embedded into the woman image invisibly into random locations using the Fibonacci-Lucas transformation [11] and then the watermark is successfully retrieved after the image is subjected to different attacks. The Fibo-Lucas transformation, in this experiment, ensures security of the watermark against unauthorised retrieval/modification along with the other desirable properties. The results of the experiments show that the procedures are robust against all the attacks. Anonymity is a method of secret communication where the transmitter and the receiver remain anonymous so that a third party, who is interested on the information but is not a legitimate user of the information, looses track of it.

- Steganography Techniques are broadly classified into two categories such as spatial domain techniques and

transform domain techniques. The more popular spatial domain methods take advantage of the human visual system and directly embed data by manipulating the pixel intensities. In transform domain procedures, the image is first transformed into frequency domain and then the message is embedded. The transform domain procedures are more robust against statistical attacks and manipulations in comparison to the spatial domain methods but spatial domain techniques are more popular due to their simplicity and ease of use. Depending upon the embedding and extraction procedures used Steganographic systems can again be classified into the following three different categories [13]: A. Pure Steganography (or No Key Steganography - NKS): This is the simplest and weakest form of Steganography in which the secret message is directly embedded into the cover image without any encryption. The success of this hidden communication depends upon the assumption that parties other than the intended receivers (attackers) are not aware of the existence of the secret message within. B. Secret Key Steganography (SKS): In this form of Steganography, both the receiver and transmitter have common agreed upon secret keys. The secret message is embedded into and extracted out of the stego image using these keys. The keys can be separately shared between both parties using some confidential channel prior to the actual transmission starts. The strength of this system is its higher security. Parties other than the intended receiver cannot retrieve the secret message or will require very high computational time and power to retrieve it applying some brute force methods, in case they suspect the presence of the secret information. The robustness of this system, of course, lies with the secrecy of the keys and the difficult part in this method is how to share the keys between the transmitting and receiving parties maintaining their secrecies. C. Public Key Steganography (PKS): This methods use a pair of public and private keys to hide the secret information. The key benefits of this system are its robustness as well as easy key management. The method is robust because the parties other than the intended receivers need to know both the private and public keys used for embedding and the encryption algorithms used, in order to be able to extract the hidden information.

## 2.3 MATERIALS AND METHODS

The work presented in this study consists of three major modules:

1.Input data.

2.Logistic maps.

3.Arnold map

4.Data Embedding.

5.Decryption

6.Final output

MODULE DESCRYPTION

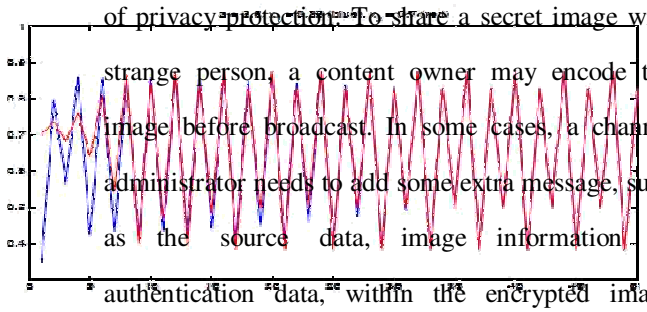
INPUT

The input image is which is to be used is stored in the database and the secret data which is to be embedded in to it is also stored in the database. The stored data is then sent for processing for data hiding.

ENCRYPTION

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, 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. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users. Encryption is an effective means of privacy protection. To share a secret image with strange person, a content owner may encode the image before broadcast. In some cases, a channel administrator needs to add some extra message, such as the source data, image information or authentication data, within the encrypted image however he does not know the original image content. It may be also expected that the original content can be recovered with-out any error after decryption and retrieve of extra message at receiver end. That means a reversible data hiding method for encrypted image is advantageous.



LOGISTIC MAP

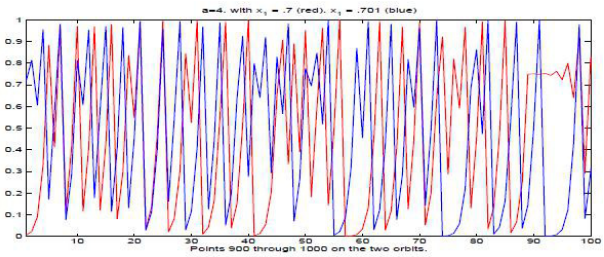
The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how complex, chaotic behaviour can arise from very simple non-linear dynamical equations. Logistic map is used to generate chaotic sequence .It is denoted as :

**xn+1=rxn(1-xn)**

where xn is a number between zero and one that represents the ratio of existing population to the maximum possible population. The values of interest for the parameter r those in the interval [0,4].

The relative simplicity of the logistic map makes it a widely used point of entry into a consideration of the concept of chaos.A rough description of chaos is that chaotic

systems exhibit a great sensitivity to initial conditions property of the logistic map for most values of r between about 3.57 and 4.Suppose we consider another initial condition, say x1 = 0.7 for the case a = 3.5. In Fig 4, we plot the first 50 points for the ICs x1 = 0.35, and x1 = 0.7. It can be shown that this convergence occurs for any initial condition in the interval (0, 1). On the other hand, consider two nearly identical (x1




.0.7, x1 = 0.701) initial conditions for the parameter value a = 4: Here is our first example of what is

called chaotic behaviour, which is often thought of as sensitive dependence.on initial conditions. In this case, even though the orbits are nearly identical at the start,after 100 points or so, there is no way to detect, either statistically or by looking at the figure, any such correlation between the two orbits.

By contrast, in the previous figure, the two orbits are completely correlated after only 50 iterations.

ARNOLD MAP :

The generalized Arnold map, with two integer control parameters a and b, this map is chaotic for all a > 0 and b > 0, because the largest Lyapunov exponent Îz=1+(ab˙ + )/2 > 1 shows the chaotic behavior of the generalized Arnold map The Arnold transform is a classical 2D invertible chaotic map defined as: The transformations are area preserving

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} mod 1$$

low period. For example a 256*256 grayscale image has a period of 192, i.e. after 192 times the shuffled image is reduced back to the original image. So an attacker only needs to manually check for a maximum of 192 times by reversing the mapping and visually verifying the image. A new image is produced when all the points in an image are manipulated once by equation (1). Arnold Cat Map (ACM) is a simple but powerful transform and digital image encryption can be achieved by applying this in the following manner [7]: Let p be the transform period of an N * N digital image I. Applying ACM for a random iteration of t times (t [1, p]) to I, a scrambled image I‘ is obtained which is completely chaotic and is different from I. Now I‘ can be transmitted over the communication channels without revealing any information to the unauthorized receivers or sniffers. At the receiving end the process is repeated for times to obtain back the original image. Figure.2 shows the results of Arnold transformation applied to a grey scale Lena image

DATA EMBEDDING

An embedded database system is a database management system (DBMS) which is tightly integrated with an application software that requires access to stored data suchthat the database system is "hidden" from the application end-user and requires little or no ongoing maintenance. Initializes some parameters, which are used for sub-sequent data pre processing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message, then the data hiding is performed on the selected regions. Finally, to obtain the stego image, it does post processing. Otherwise the scheme needs to revise the parameters, and then repeats region selection and capacity estimation until can be embedded completely. May be the parameters are different for different image content and secret message .

EXTRACTING DATA

First extract the side information, i.e., the block size and the threshold from the stego image. As we done exactly the same things in data embedding. The stego image is divided into blocks and the blocks are then rotated by random degrees based on the secret key. The resulting image is rearranged as a row vector . Finally, we get the embedding units by dividing into no overlapping blocks with two consecutive pixels.

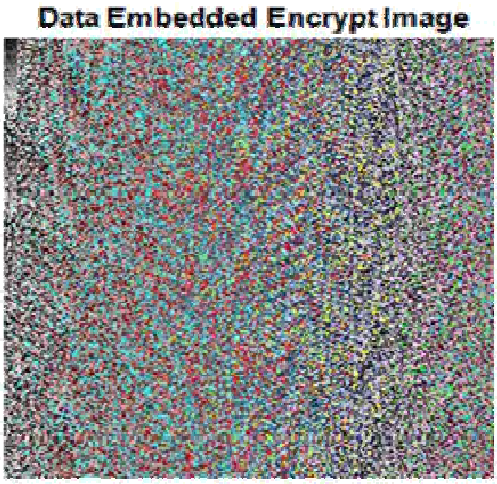
DECRYPTION

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or

automatically. It may also be performed with a set of keys or passwords

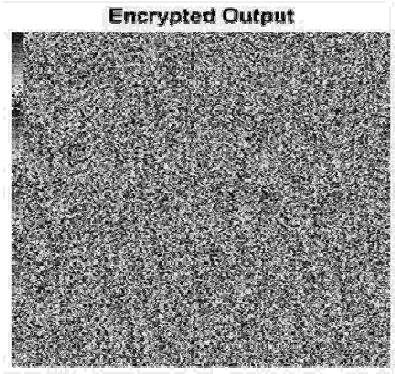
FINAL OUTPUT

*The final output is decrypted output.*

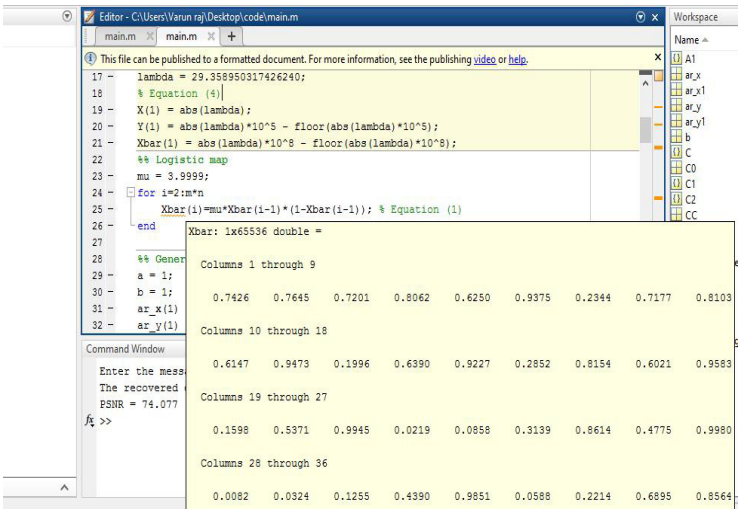



### 2.3.2 SIMULATED OUTPUT





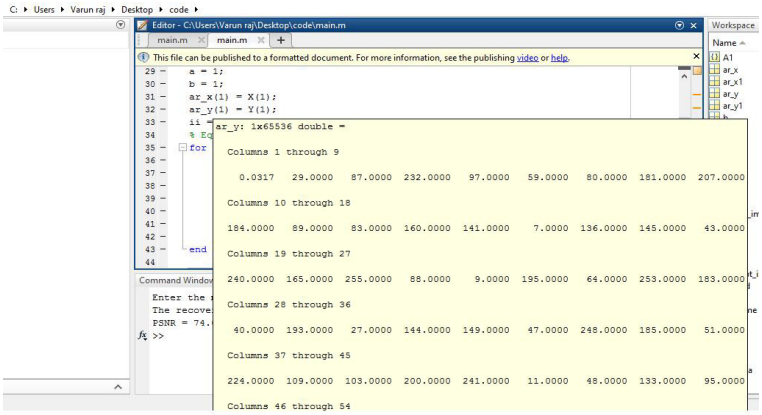
LOGISTIC MAP SEQUENCE :-

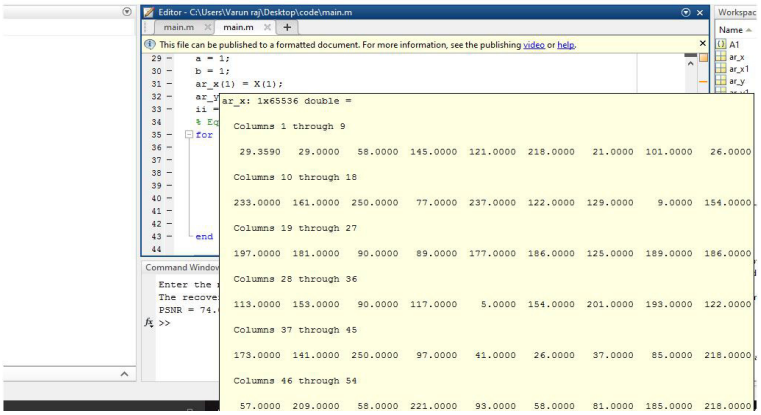



COMPARSION OF PSNR

| COVER IMAGE | REFERENCE 1 | REFERENCE 2 | REFERENCE 3 | REFERENCE 5 | REFERENCE 6 | THE PROPOESD METHOD |
|---|---|---|---|---|---|---|
| LENA | 39.20 | 41.60 | 40.37 | 45.12 | 54.25 | 74.077 |
| PEPPER | 39.17 | 41.56 | 39.30 | 43.13 | 54.12 | 70.212 |
| BABOON | 39.18 | 41.55 | 39.94 | 45.12 | 53.97 | 65.669 |

ARNOLD MAP SEQUENCE




CONCLUSION

In this work, We dealt with the techniques for steganography as related to colourimage. A new and efficient stenographic method for embedding secret message into images without producing a major changes has been done in our project. This property enables the method to avoid steganalysis. This method is also capable of extracting the secret message without the cover image. Also, the researchers can hide a large number of char inside the selected cover image. Experimental results showed that the proposed method gave the best values for PSNR, which means that there is no difference between the original and the Stegoimages. The limitations in our project is when we do encryption process ,we have to combine the sequences of input image ,logistic map sequence and Arnold sequence ,so the size of the encrypted image may increase. When Com-pared with proposed method our method

is more efficient and highly secured ,because in proposed method they used one map for encryption .In our method we use two maps for encryption .The Quality of the image also increased ,which gives high PSNR in our method

REFERENCES

1. Alatas B (2010) Chaotic harmony search algorithms. Appl Math Comput 216:2687â˘A ¸S2699

2. Arsalan M, Malik SA, Khan A (2012) Intelligent reversible watermarking in integer
wavelet domain for medical images. J SystSoftw 85(4):883â˘A ¸S894

3. Baykasoglu A (2012) Design optimization with chaos embedded great deluge
algorithm. Appl Soft Comput 12:1055â˘A ¸S1067 123

4. Bender W, Paiz FJ, Butera W, Pogreb S, Gruhl D, Hwang R (2000) Applications
for data hiding. IBM Syst J 39(3â˘A ¸S4):547â˘A ¸S568

5. Bhowal K, Pal AJ, Tomar GS, Sarkar PP (2010) Audio steganography using GA.
In: International conference on computational intelligence and communication
networks, pp 449â˘A ¸S453

6. Caponetto R, Fortuna L, Fazzino S, Gabriella M (2003) Chaotic sequences to
improve the performance of evolutionary algorithms. IEEE Trans EvolComput
7:289â˘A ¸S304

7. Chambers LD (2001) The practical handbook of genetic algorithms: applications.
Chapman Hall/CRC, Boca Raton

8. Chan CK, ChengLM(2004) Hiding data in images by simple LSB substitution.
Pattern Recogn 37(3):469â˘A ¸S474

9. Chang CC, Lin CY, Fan YH (2008) Lossless data hiding for color images based
on block truncation coding.

10. Chang CC, Hsieh YP, Lin CH (2008) Sharing secrets in stego images with authentication.
Pattern Recogn41(10):3130â˘A ¸S3137

11. Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T (2008) Digital watermarking
and steganography. In: The Morgan Kaufmann series in multimedia information
and systems

12. Dasgupta K, Mondal JK, Dutta P (2013) Optimized video steganography using
genetic algorithm (GA). ProcediaTechnol 10:131â˘A ¸S137

13. Drâ˘A ´ Zeo J, Pâ˘A ´ Zetrowski A, Siarry P, Taillard E (2006) Metaheuristics for hard
optimization. Springer, Berlin Elattar EE (2015)

14. A hybrid genetic algorithm and bacterial foraging approach for dynamic economic
dispatch problem. Int J Electrical Power Energy Syst 69:18â˘A ¸S26

15. Elshoura SM, Megherbi DB (2013) A secure high capacity full-gray-scale-level
multi-image information hiding and secret image authentication scheme via Tchebichef
moments. Sig Process Image Commun28:531â˘A ¸S552

16. El-Emam NN (2015) New data-hiding algorithm based on adaptive neural networks
with modified particle swarm optimization. ComputSecur 55:21â˘A ¸S45
37

17. Ghebleh M, Kanso A (2014) A robust chaotic algorithm for digital image steganog18. Huang G, Cambria E, Toh K, Widrow B, Xu Z (2015) New trends of learning in
computational intelligence. IEEE ComputIntell Mag 10(2):16â˘A ¸S17

19. Jawad K, Khan A (2013) Genetic algorithm and difference expansion based reversible
watermarking for relational databases. J SystSoftw 86(11):2742â˘A ¸S2753

20. Kanan HR, Nazer B (2014) A novel image steganography scheme with high embedding
capacity and tunable visual image quality based on a genetic algorithm.
Expert SystAppl 41:6123â˘A ¸S6130
21. Kanso A, Own HS (2012) Steganographic algorithm based on a chaotic map.
Commun Nonlinear SciNumerSimul 17(8):3287â˘A ¸S3302
22. Khan A, Malik SA, Ali A, Chamlawi R, Hussain M, Mahmood MT, Usman I
(2012) Intelligent reversiblewatermarking and authentication: hiding depth map
information for 3D cameras. InfSci 216:155â˘A ¸S175
23. Khan MK, Zhang J, Tian L (2007) Chaotic secure content-based hidden transmission
of biometric templates.ChaosSolitons Fractals 32(5):1749â˘A ¸S1759
24. Khodaei M, Faez K (2010) Image hiding by using genetic algorithm and LSB
substitution. Image Signal Process Lecture NotesComputSci 6134:404â˘A ¸S411
25. Kim T, Lee K, Baik J (2015) An effective approach to estimating the parameters
of software reliability growth models using a real-valued genetic algorithm. J
SystSoftw 102:134â˘A ¸S144
26. Kuo RJ, Syu YJ, Chen ZY, Tien FC (2012) Integration of particle swarm optimization
and genetic algorithm for dynamic clustering. InfSci 195:124â˘A ¸S140
27. Kurban T, Civicioglu P, Kurban R, Besdok E (2014) Comparison of evolutionary
and swarm based computational techniques for multilevel color image thresholding.
Appl Soft Comput 23:128â˘A ¸S143
28. Li X, Wang J (2007) Asteganographic method based upon JPEG and particle
swarm optimization algorithm. InfSci 177(15):3099â˘A ¸S3109
29. Lin CC, TsaiWH(2004) Secret image sharing with steganography and authentication.
J SystSoftw 73(3):405â˘A ¸S 414
30. [32] Liu Z, Zhang Y, Liu W, Meng F, Wu Q, Liu S (2013) Optical color image
hiding scheme based on chaotic mapping and Hartley transform. Opt Lasers Eng
51(8):967â˘A ¸S972
31. Nian-ShengL(2011) Pseudo-randomness and complexity of binary sequences generated
by the chaotic system. Commun Nonlinear SciNumerSimul 16(2):761â˘A ¸S768
32. Roy R, Sarkar A, Changder S (2013) Chaos based edge adaptive image steganography.
ProcediaTechnol 10:138â˘A ¸S146 123
38
33. A new data hiding method based on chaos embedded...Schaefer R (2007) Foundations
of global genetic optimization. Springer, Berlin
34. SuneelM(2006) Chaotic sequences for secure CDMA, Ramanujan Institute for
Advance Study in Mathematics, pp 1â˘A ¸S4
35. Tataru RL, Battikh D, El Assad S, Noura H, Deforges O (2012) Enhanced adaptive
data hiding in spatial LSB domain by using chaotic sequences. In: Eighth
international conference on intelligent information hiding and multimedia signal
processing (IIH-MSP), 2012, pp 85â˘A ¸S88
36. Tu TY, Wang CH (2015) Reversible data hiding with high payload based on referred
frequency for VQ compressed codes index. Sig Process 108:278â˘A ¸S287
37. Verma OP, Kumar P, Hanmandlu M, Chhabra S (2012) High dynamic range optimal

fuzzy color image enhancement using artificial ant colony system. Appl Soft
Comput 12(1):394â˘A ¸S404
38. Wang RZ, Lin CF, Lin JC (2001) Image hiding by optimal LSB substitution and
genetic algorithm. Pattern Recogn 34(3):671â˘A ¸S683
39. Wu CC, Kao SJ, Hwang MS (2011) A high quality image sharing with steganography
and adaptive authentication scheme. J SystSoftw 84(12):2196â˘A ¸S2207
40. Yang CN, Chen TS, Yu KH, Wang CC (2007) Improvements of image sharing
with steganography and authentication. J SystSoftw 80(7):1070â˘A ¸S1076