Nat. Volatiles & Essent. Oils, 2021; 8(5): 10391-10400

NVEO
Natural Volatiles &
Essential Oils

Image Encryption Method by Using Chaotic Map and DNA Encoding

Dr. Aditya Pai H[1,*], Dr. Piyush Kumar Pareek[2], Dr. Guru Prasad M.S[3], Prabhdeep Singh[4], Dr.Bhagavant K. Deshpande[5]

[1]Associate Professor, Dept of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun – 248002
[2]Professor and Head of IPR Cell, Nitte Meenakshi Institute of Technology, Bengaluru – 56006
3Dept of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun – 248002
[4]Dept of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun – 248002
[5]Dept of Computer Science and Engineering, Graphic Era Hill University, Dehradun – 248002

Abstract

Confidentiality of image files is a daunting task these days for a variety of reasons in diverse sectors namely in medical, defense, academics and many more. A variety of practical techniques are investigated in past years to protect pictures data but, such existing methods have certain limitations in present systems due to technical advancements. Several researchers have looked at a variety of methods as well as strategies for maintaining image secrecy and protecting top secret information against attackers during the transfer of images throughout communications infrastructure. In this article, a novel image encryption algorithm based on chaotic map as well as the DNA encoding jointly utilized for images encryption in a more pragmatic manner as required in modern world to secure confidential data. This method was tested and verified using the MATLAB R2020a version installed in a personal laptop having system specifications of 64-bit operating system, Window 10 and 16 GB RAM (Random Access Memory). For numerous selected images for testing, the outcomes of this proposed method indicate the best NPCR (Number of Pixel Change Rate) as well as UACI (Unified Average Changed Intensity) scores. This algorithm performs with a number of pictures formats and is in high demand in modern world for securing sensitive data or information throughout transmission via communications infrastructure. In future, there is mammoth scope for more investigations in order to find pragmatic solutions as the modern communication systems are changing rapidly worldwide due to the technological advancements.

Keywords: Communication, Data, Encryption, Information, Image, NPCR, UACI

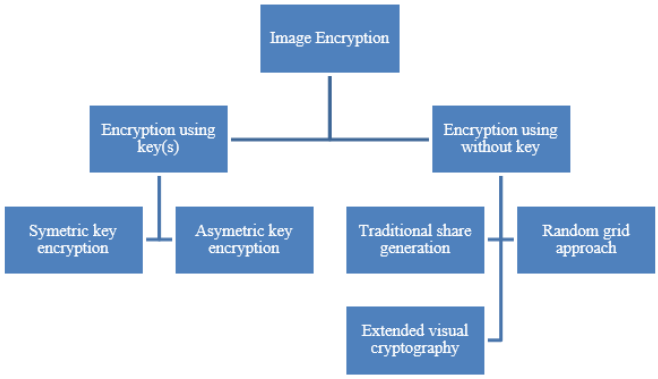
Introduction

Due to a plethora of countered problems as well as the sharing of pictures over the web via communications medium, digital picture security has now become incredibly hard and overwhelming around the world. During delivery, picture confidentiality is an essential but main priority, and many approaches have been investigated to protect data packets through communications infrastructure. Data encryption including verification are enormous obstacles that people are facing globally[1]. This is very intricate as well as critical to analyze and test several innovative approaches for protecting sensitive data during communication for securing the confidential data from diverse attackers. Various researchers have looked at numerous techniques towards data protection, namely the cryptography, which is a valuable strategy to securing confidential information and minimizes the likelihood of unauthorized access throughout communication[2].

One of the most critical facets of correspondence is data or information protection, which requires more attention to secure confidential information. The safety of the photos is much more difficult as they are broadcast. The metadata for photographs differs from those of other data forms namely the text, audio, video, and so on. Where critical but equal data is transferred through one side to another by people in the

context of photos or document, secure algorithms are necessary. When sensitive data or information is exchanged through a communication medium, traditional cryptographic approaches and practices play a crucial role in ensuring its protection. The image content is incredibly important to safeguard against attackers because it provides a wealth of vital knowledge. There seem to be a variety of file formats which contain a lot of important information that can be transmitted through social networks[3], [4]. Fig. 1 represents the classification of image encryption approaches.

Figure 1. Illustrates the classification of image encryption approaches



The technology sector, where a limited division of numerous digital picture apps is becoming overwhelmingly prevalent, has come to represent a central role globally as research, engineering, as well as culture have progressed. Advantages of electronic have been the most widely utilized media forms, with applications in areas as diverse as diplomacy, finance, security, including schooling. Picture transmission protection, on other hand, is vulnerable due to transparent existence of diverse channels. Digital photographs must also satisfy the top levels of secrecy in these respects, including defense policy, banking, including healthcare. As a result, picture strong encryption has proven to be an efficient method of protecting photographs during transmission[5].

Literature review

Azam et al. found new form of encryption algorithm based upon on AES (Advanced Encryption Standard) as well as phase embedding methods. These writers conducted a more precise as well as simple picture encryption analysis. In the verification of diverse data, the sensitive picture is scattered with both the fuzzily specified RTS. The above method is a strategic means of deciphering images because it has a function that provides high confidentiality as well as hassle-free decoding. Throughout this report, the review looks at a quick authentication scenario[6]. Pak et al. used a modification of received outcome orders of both of the two adjacent remaining 1-D chaotic map to explore recent method for designing a modified, advanced as well as functional chaotic structure. This proposed technique is much more advanced than current pictures encryption algorithms which are investigated through a variety of investigators across last decade. In contrast to traditional approaches, the computation and output specifications of the whole training methodology indicate here that approach for pictures authentication is simpler to implement. The research team discovered that now this suggested solution provides the optimal degree of precision including confidentiality for sensitive digital colour picture data throughout delivery over social networks[7].

Mirzaei et al. explored a new pictures encryption approach which is based upon the total shuffling approach as well as another innovative parallel encryption approach jointly in order to offer extensive secrecy to the pictures confidential information. In order to, puzzle diverse attackers in a pragmatic manner, throughout image transfer via wireless networks, two different schemes were used for

efficient image transmission. The selected plain photos have been subdivided into four photos throughout this process, as well as the location of each divided image was modified at randomly according to logistic map. In terms of anonymity for different image sizes throughout delivery over communication infrastructure, such suggested technique is more sophisticated than previous methods. The writers discovered that the current approach is faster, safer, stable, and more accurate than some other approaches [8].

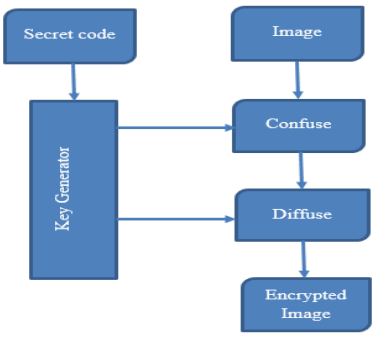
Sankpal et al. carried out a literature assessment on previous image encryption approaches explored via multifarious researchers to offer a comprehensive overview of technologies and procedures used to encrypt photographs. In past decade, confidential data transfer via communication networks has increased significantly. When such mammoth data or information is transferred via communication networks without utilization of efficient encryption methods, there are gigantic risks of information or data being leaked by the attackers. Multimedia apps have included images for knowledge sharing in addition to making the collaboration activities more efficient. Other photo encryption approaches, namely AES as well as the DES (Data Encryption Standard), and many more have also been investigated, but each has its own set of limitations. As a result, novel and efficient image encryption techniques are in high demand[9].

Methodology

Design

In present era, photograph authentication is becoming extremely necessary from the standpoint of privacy. Quite few image preservation measures have been explored to prevent personal data of the diverse pictures from attackers. In this article, a recent photograph encryption approach based on chaotic map as well as the DNA encoding mutually utilized for pictures encryption in a more realistic mode as mandatory in contemporary world to secure confidential information's. Fig. 2 depicts the block diagram of our suggested model. The images encryption strategies have a wide demand since multiple files or photographs take complex data or facts. In order to, effectively analyze diverse kinds of existing issues, authors explored the prior art before analyzing this design strategy for the development of this proposed prototypical. Although, in past extensive investigations were done by the multifarious investigators but the current issue was the inefficient and insecure data transmission via large social networks that is becoming the major threat in the contemporary world continuously. After analyzing multifarious open literature, authors explored this suggested model for improving the confidentiality of the images in communication with high degree of the precision.

Figure 2. Illustrates the block diagram of our suggested model.



Instrument

This whole experiment was done utilizing MATLAB R2020a activated on a laptop that have the following system configuration; 64-bit of the operating system as well as 16 GB of Random Access Memory (RAM). MATALB software package has been found most powerful and highly demanded tool in modern era for a variety of purposes. Within this software package, there are multifarious valuable tools that are offering constructive features to address various issues. Many scientists choose MATLAB to other tools as it comprises of the user-friendly GUI (Graphical User Interface) as well as lower computational uncertainty. MATLAB is utilized for a multitude of scenarios.

Data Analysis

The security of protected data found in different image formats necessitates the confidentiality of photographs. Using such unwanted noise signals, some attackers could break personal details through communication channels. Data confidentiality is a major concern in a variety of fields, including surveillance, defense, and others. The said suggested methodology is a practical way to protect secrecy without reducing the risk of security breaches. Since it requires various keys for encryption as well as pragmatic decryption procedures, due to that our suggested methodology based on DNA encoding as well as chaotic map procedures is asymmetric. There are taken diverse equations in order to evaluate the corresponding values of the certain parameters as mentioned herein for evaluation procedure.

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255} \right] \times \frac{100\%}{M \times N}$$

The MAE (Mean Absolute Error) could be assessed by utilizing this following equation.

$$MAE = \frac{1}{W \times H} \sum_{i=1}^{H} \sum_{j=1}^{W} |p(i,j) - E(i,j)|$$

Correlation coefficients could be explored by utilizing these subsequent expressions.

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Herein, the$C(x,y), D(x)$ as well as$D(y)$ could be accessed through these following expressions;

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K} \sum_{i=1}^{K} (x_i - E(x))^2$$

$$D(y) = \frac{1}{K} \sum_{i=1}^{K} (y_i - E(y))^2$$

There is another pragmatic as well as significant parameter namely the MSE (Mean Square Error) in analysis of different photos formats. The MSE could be evaluated utilizing following formula.

$$MSE = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[P(i,j) - E(i,j)]^2}{W \times H}$$

The acquired plain-text data sets were encrypted by assigning secret code words at the transmission site, as well as the plain-text data is acquired via decrypting received cipher-text using its own assigned private code. These aforementioned diverse equations were used for measuring the various parameters namely NPCR (Number of Pixels Change Rate) as well as UACI (Unified Average Change Intensity), and many more.

Algorithm

Assumption: It is supposed that selected picture *Y* overall dimension are considered$K \times L$, then the procedure steps for encryption are illustrated as:

Step First*:* To transform real picture *Y*in in 2-D Matrix.

Step Second*:* To originate two diverse kind of 1-D descending index series utilizing logistic map for confuse photo.

Step Third*:* To exchange the confused photo within 2-D matrix and furthermore originate random integer.

Step Fourth*:* To originate storage unit through utilizing Chebyshev mapping.

Step Fifth*:* To originate new arbitrary integer that is utilized for deciding the DNA scrambling method.

Step Sixth*:* At last, transform 2-D matrix in the encrypted photograph as well as outcome would be encrypted version of the applied photograph.

Results and discussion

The actual test photos chosen for the experiment are seen in Fig. 3. In order to achieve the desired outcomes, four multifarious pictures of equal dimension with pixel values of 128× 128 were chosen for verification and analysis. Lena, Peppers, Cameraman, and Baboon are the four images chosen. The coded versions including all chosen photos, specifically Lena, Peppers, Cameraman, and the Baboon, are seen in Fig. 4. The suggested algorithms were used to encode all photos to achieve quicker performance than conventional methods. The deciphered representations of all photos on the receiver end are illustrated in Fig. 5.

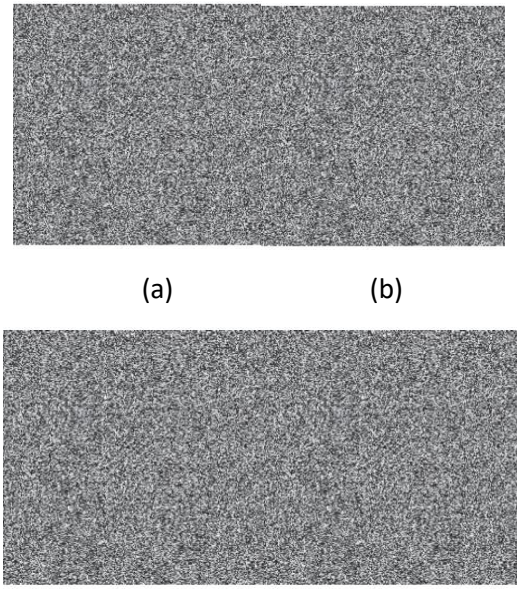
Figure 3. Illustrates original test images selected for experiment. Plain pictures of (a) Lena (b) Peppers (c) Cameraman (d) Baboon.

(a) (b)

(c) (d)

For the encryption as well as decryption procedures, chaotic map as well as the DNA encoding jointly utilized and measured results is optimal. For each photo, Table I summarizes the measured NPCR (Number of Pixel Changes Rate) as well as the UACI (Unified Average Changing Intensity) values. These NPCR as well as UACI scores for Lena, Peppers, the Cameraman, and the Baboon are 99.8122, 99.8032, 99.8043, 99.8129 and 33.4611, 32.4715, 33.4719, 33.4724, respectively. Table II shows assessment of diverse correlation coefficients (CC) of selected Lena photograph. The diagonal, vertical and horizontal correlation coefficients of real photographs and encrypted photos are 0.9538, 0.92940, 0.9861 and -0.0033, 0.0025, 0.0003, respectively.

Figure 4. Illustrates encrypted pictures of (a) Lena (b) Peppers (c) Cameraman (d) Baboon



(a) (b)

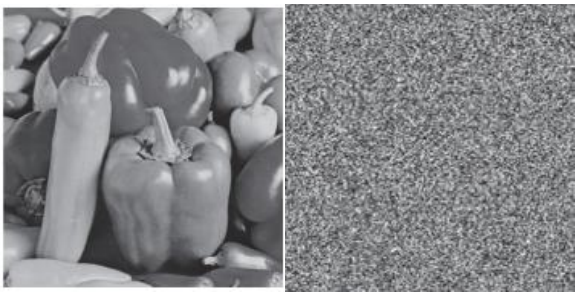
(c) (d)

Figure 5. Illustrates decrypted pictures of (a) Lena (b) Peppers (c) Cameraman (d) Baboon.

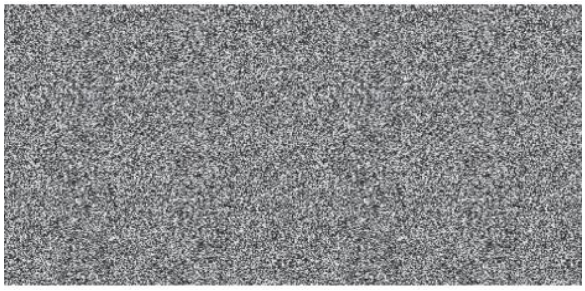
(a) (b)

(c) (d)

Figure 6. Illustrates original and corresponding decrypted selected picture of Baboon. The selected Baboon picture was encrypted by two separate code words c1 and c2. (a) Real picture, (b) Encrypted picture through code c1, (c) Encrypted picture through code c2, (d) Difference picture of (b) and (c), (e) Decrypted picture through incorrect code c1, (f) Decrypted picture by correct code c2.



(a) (b)



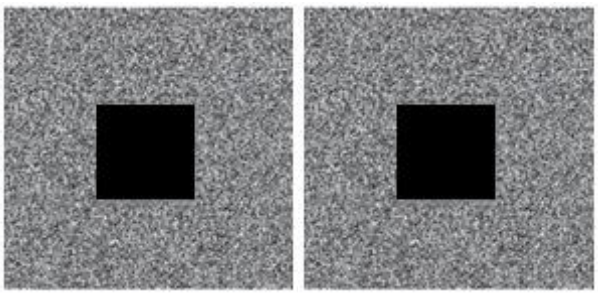
(c) (d)

(e) (f)

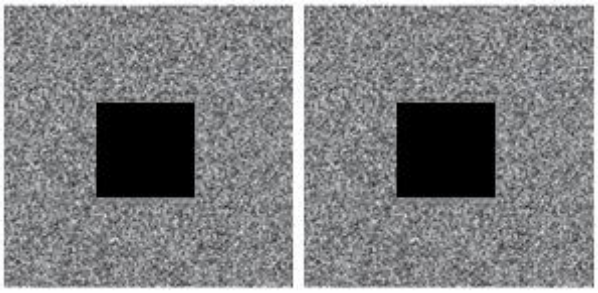
The biggest concerns when transmitting photographs through communication networks is to maintain and preserve the photos confidentiality. The secrecy of photographs is getting more complex in contemporary world for a variety of reasons. By assigning various code words to diverse photographs for confusing attackers, this proposed DNA encoding approach with chaotic map jointly operation-based algorithm provides highest protection for multifarious photographs formats. The initial photograph of

Peppers as well as the de-ciphered selected photograph of Peppers are seen in Fig. 6, as well as this selected Peppers photograph was encoded with two separate code words c1 and c2 for confusing attackers. Figure 7 demonstrates (a) encrypted photo of Lena (b) encrypted photo of Peppers (c) encrypted photo of Cameraman (d) encrypted photo of Baboon (e) photo (a) decryption (f) photo (b) decryption (g) photo (c) decryption (h) photo (d) decryption. This suggested algorithm is offering the highest level secrecy in comparison to existing approaches as well as this is more robust and secure against the cropping assault in the middle fragment of the photo. This analysis is depicting the cropping on 0.125% portion of the photo in the center of overall photo segment.

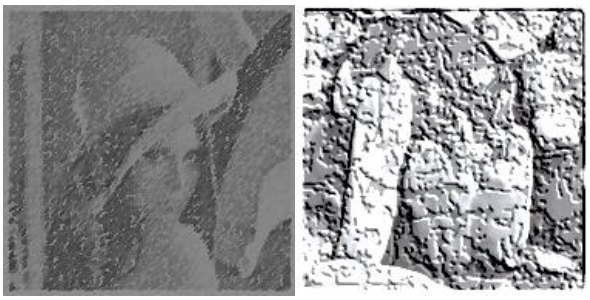
Figure 7. Depicts (a) encrypted photo of Lena (b) encrypted photo of Peppers (c) encrypted photo of Cameraman (d) encrypted photo of Baboon (e) photo (a) decryption (f) photo (b) decryption (g) photo (c) decryption (h) photo (d) decryption.



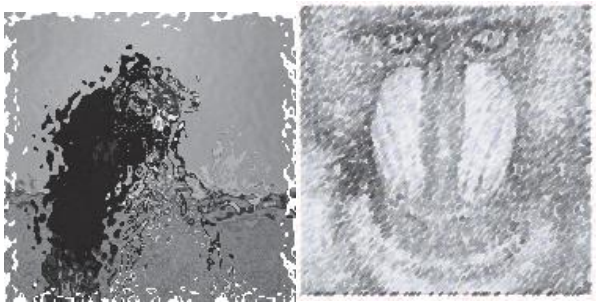
(a) (b)



(c) (d)



(e) (f)



(g) (h)

Table 1 The NPCR and UACI values of selected test images.

S. No.	Picture(s)	NPCR (%)	UACI (%)
1	Lena	99.8122	33.4611
2	Peppers	99.8032	32.4715
3	Cameraman	99.8043	33.4719
4	Baboon	99.8129	33.4724

Table 2 Assessment of diverse correlation coefficients (cc) of selected lena photograph

S. No.	Correlation Coefficient (CC)	Diagonal	Vertical	Horizontal
1	Real Photograph	0.9538	0.9240	0.9861
2	Encrypted Photograph	-0.0033	0.0025	0.0003
3	Zhang et al.[10]	0.0039	0.0023	0.0036

Conclusion

In recent times the secrecy of the photographs data is continuously becoming a gigantic concern in modern era as certain photos comprises diverse kind of essential data in multifarious formats. In order to, secure photographs at delivery time via communication networks, a recent approach were explored by utilizing the DNA encoding as well as the chaotic maps jointly to find out a pragmatic solution of existing issues that are encountered by multifarious investigators. This research presents an efficient and novel photo encryption approach that is more safe and robust against noise attacks in data communication in order to secure sensitive data. Because of its low computational complexity as well as ease of equipment implementation, such photo encryption algorithm is well suited for real time applications. This experiment was carried out with high precision for eliminating the chances of the error and to validate the measured results in an efficient manner. For the experimentation, a personal laptop was utilized installed with MATLAB R2020a version that comprising of the following system specifications: 16 GB of the RAM (Random

Access Memory), Window 10 installed with 64 bit operating system (OS). The measured score of NPCR as well as UACI for every selected photograph are 99.8122, 99.8032, 99.8043, 99.8129 and 33.4611, 32.4715, 33.4719, 33.4724, respectively. Furthermore, this analysis is depicting the cropping on 0.125% portion of the photo in the center of overall photo segment. In comparison to conventional approaches, the results show that this approach is pragmatic and more reliable. Numerous studies have been conducted in this area, but further investigations are needed to fully explore this sector's potential as well as produce better results according to modern systems requirements due to technical advancements.

REFERENCES

A. U. Rehman, H. Wang, M. M. A. Shahid, S. Iqbal, Z. Abbas, and A. Firdous, “A Selective Cross-Substitution Technique for Encrypting Color Images Using Chaos, DNA Rules and SHA-512,” IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2951749.

Y. Hashemi, “Design a New Image Encryption using Fuzzy Integral Permutation with Coupled Chaotic Maps,” Int. J. Res. Comput. Sci., 2013, doi: 10.7815/ijorcs.31.2013.058.

C. Zhu, Z. Gan, Y. Lu, and X. Chai, “An image encryption algorithm based on 3-D DNA level permutation and substitution scheme,” Multimed. Tools Appl., 2020, doi: 10.1007/s11042-019-08226-4.

X. Zhang, Z. Zhou, and Y. Niu, “An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding,” IEEE Photonics J., 2018, doi: 10.1109/JPHOT.2018.2859257.

R. Enayatifar, F. G. Guimarães, and P. Siarry, “Index-based permutation-diffusion in multiple-image encryption using DNA sequence,” Opt. Lasers Eng., 2019, doi: 10.1016/j.optlaseng.2018.11.017.

N. A. Azam, “A novel fuzzy encryption technique based on multiple right translated AES gray s-boxes and phase embedding,” Secur. Commun. Networks, 2017, doi: 10.1155/2017/5790189.

C. Pak and L. Huang, “A new color image encryption using combination of the 1D chaotic map,” Signal Processing, 2017, doi: 10.1016/j.sigpro.2017.03.011.

O. Mirzaei, M. Yaghoobi, and H. Irani, “A new image encryption method: Parallel sub-image encryption with hyper chaos,” Nonlinear Dyn., 2012, doi: 10.1007/s11071-011-0006-6.

P. R. Sankpal and P. A. Vijaya, “Image encryption using chaotic maps: A survey,” 2014, doi: 10.1109/ICSIP.2014.80.

Q. Zhang, L. Guo, and X. Wei, “Image encryption using DNA addition combining with chaotic maps,” Math. Comput. Model., 2010, doi: 10.1016/j.mcm.2010.06.005.