AN EFFICIENT CHAOTIC IMAGE ENCRYPTION METHODS

ALAWODE, Ademola J. & AROWOLO, Paul O.
Department of Computer Science, The Federal Polytechnic, Ilaro
ademola.alawode@federalpolyilaro.edu.ng paul.arowolo@federalpolyilaro.edu.ng

Abstract

The advent of digital communications, both inside and outside the home-office environment has brought increased demand for effective encryption systems. When there is no strict relationship between the cipher and the original data and the ability to recreate the original image, the purpose of encryption technology becomes more apparent. Chaotic systems can be used to achieve the encryption because they are known to be more random and unpredictable. Because of their intricate dynamic features, such as diffusion and chaos, chaotic economic systems have received a lot of attention in literature. To hide the identity of the source image, chaos-based image encryption algorithms rearrange the position of the pixels and spread their values. The placements of the pixels were altered in this investigation to lessen the association between neighboring pixels by changing both the pixel's position and its value. By using the key produced by the dyadic transform to encrypt the scrambled pixels, the encrypted image is created. In the distribution of the encrypted image's pixel values, the results showed unpredictable behavior. Since the cryptosystem is diffusion-based and secure, it is easy to use and quick for real-time transmission.

Keywords: Chaotic, Encryption, Algorithms, Digital Communication

Introduction

Information and communication technologies (ICTs) is a more inclusive term for information technology (IT), which includes all media applications and services that allow users to access, retrieve, store, transmit, and manipulate information in a digital form. Examples of ICTs include the internet, wireless networks, cell phones, computers, software, middleware, video conferencing, social networking, and other media. ICTs also refer to a unified system of cabling (including signal distribution and administration) or connection system that enables the integration of media technologies, such as audio-visual and telephone networks with computer networks.

The common description of the information "haves" and "have-nots" implies that ICTs are about much more than just access to information or computer technology. Access to information, people, services, and technology is shaped by ICTs for an individual, a household, a business, or a country. Information, people, services, and technology are four interconnected resources that can all be accessed differently depending on the social and technological decisions made concerning ICTs.

Access to information is the most well-known. ICTs modify not only how people obtain information but also the totality of what a person knows and the information that is available to a person at any given time and location. ICTs contribute to the disparity between those who have access to information and those who do not. Multimedia, which includes music, video, and graphics, has developed quickly in recent years. Additionally encouraging the widespread use of digital information are computer science and network technologies.

Among these forms of multimedia, photographs serve as a useful tool for comprehending color, which is crucial in everyday life. However, there appears to be a lack of security for exchanging photos over the network, especially some confidential photographs like medical and military images, because of unauthorized wiretapping, alteration, or interception. Symmetric and asymmetric cryptography are the two categories into which cryptography is structurally divided. It has given rise to a large number of efficient ciphers for user data, notably text. We favor symmetric cryptosystems for coding due to their great efficiency and minimal computational requirements.

An image has some inherent characteristics and is different from textual content, for example, enormous data, high correlation, long redundancy, and bulk data capacity. Therefore, traditional methods such as advanced encryption standard (AES), data encryption standard (DES), or international data encryption algorithm (IDEA) are not effective options for image encryption.

Chaos based image encryption is one of recently and widely used approaches to fulfill the security requirements of digital images. The chaotic systems are very sensitive to initial conditions and system parameters. For a given set of parameters in chaotic regime, two close initial conditions lead the system into divergent trajectories. Therefore, an image encryption and decryption scheme can be developed if the initial condition and parameters are chosen as keys (Lawande, et al, 2005). Since the same parameters are used for encryption and decryption, the chaos-based image encryption scheme is symmetric.

Now-a-days a huge amount of data is being exchanged over internet and about 84% of internet traffic is multimedia content such as images and videos, (Jai & Arun, 2020). Especially the digital image communication has drastically increased over past few decades and image communication has extended its application on various fields of such as military, space, research, medical science, tele-medicine, social networks, etc. Thus, process of providing security for the data sent over the open channels such as internet plays an important role to ensure confidentiality of sensitive information. The traditional algorithms such as AES, DES, RSA etc., are suitable for text but unfortunately, they don't provide considerable confidentiality when it comes to multimedia data such as image and video due to properties like spatial redundancies, data size, etc.

Aim and Objectives of the Study

The aim of the study is to develop a chaotic image encryption system that ensures security of images sent over the internet by transforming the positions of the pixels which decreases the correlation between adjacent pixels.

The following are the objectives that will be used to achieve this aim:

- To perform critical analysis of the existing image encryption techniques.
- To formulate/model mathematical algorithms that are capable of changing the position of image pixels in a non-linear pattern, as well as reverse the operation.
- To develop a system that follows the formulated mathematical algorithmic process.
- To carry out tests on the newly developed system using several software testing approaches like the white box, the black box, and the grey box testing.
- To deploy the newly developed encryption system after meeting both the functional and nonfunctional requirement of the system.

Overview of Chaotic Encrytpion

Technology advancements have made it simple to instantly exchange information like photographs, data, and speech. Since this information is shared over a single frequency band, end users may be concerned about the security of their personal data. However, a variety of encryption methods have been developed, and each has pros and cons of its own. One of these algorithms is referred to as a chaos-based cryptography algorithm. It has been suggested that this technique is effective at encrypting photos. Chaos is a good encryption algorithm because it offers quick processing, decent speed, and strong security. Despite having some chaotic behavior, this system is perfectly deterministic. We can create a confusion matrix if we are provided the beginning value and its parameters. In 1970s, Chaos theory was proposed, which was used in a number of research areas, such as mathematics, engineering, physics, biology, and so on (Schneier, 1996). The complex behavior of chaotic systems in nonlinear deterministic was described. The first description of a chaotic process was made in 1963 by Lorenz, who developed a system called the Lorenz attractor that coupled nonlinear differential equations.

Numerous chaos-based digital picture encryption systems exploiting chaotic maps have been presented in the literature since Matthews R.A. introduced the first chaos-based image encryption scheme in 1993. In recent years, chaotic encryption has gained popularity as a research area. Researchers have presented numerous image encryption techniques during the past 20 years. The most notable similarity between chaos and encryption is their sensitivity to changes in parameters and variables.

The effectiveness of a straightforward chaos-based encryption method designed specifically for photos is proposed in this paper, and its performance is examined.

For the purpose of applying the concept of confusion and diffusion to photographs, Bogdanov map-based permutation is utilized. While diffusion modifies the values of the pixels, confusion rearranges the positions of the pixels inside the image and creates a new arrangement of pixels. According to experimental findings, it is easy, quick, and reliable.

In general, most of the available traditional encryption algorithms are used for text data. Although we can use the traditional encryption algorithm to encrypt images directly, this may not be a good idea for some reasons. First, image data have their special features such as high redundancy, and high correlation among pixels. Secondly, they are usually huge in size that makes traditional encryption methods difficult to apply and slow to process. Thirdly, the decrypted text must be equal to the original text but this requirement is not necessary for image data because characteristic of human insight, a decrypted image containing small distortion is usually acceptable. However, the image encryption algorithms can be categories into three major groups.

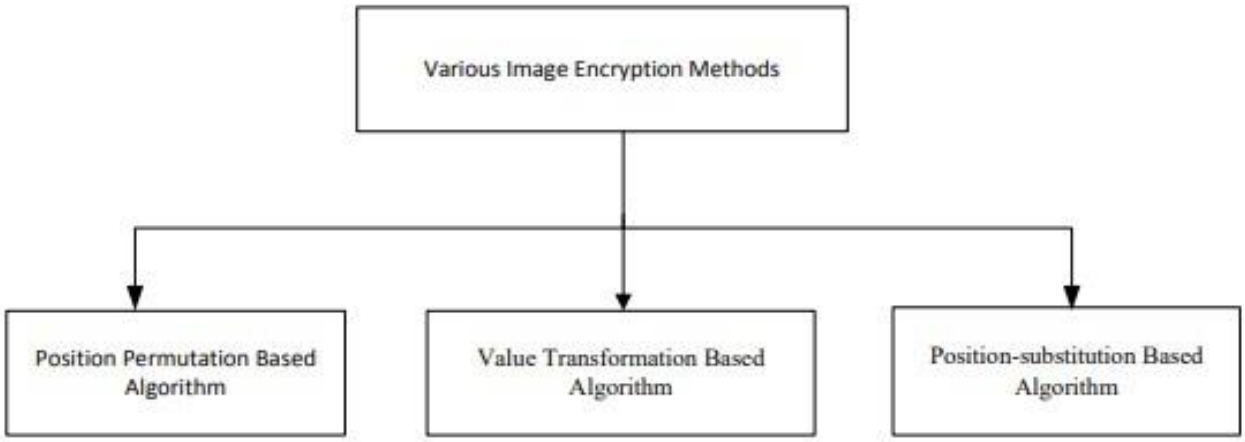


Figure 1 Various Image Encryption Methods. (Source: Gajendra, 2016)

Position Permutation (Transposition) Based Algorithm

Transposition means rearranging elements in the plain image. The rearrangement of element can be done by bit, pixel, and block wise. The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce high level security. In the bit permutation technique, the bits in each pixel are permuted using the permutation keys with the key length equal to 8. In the pixel permutation, 8 pixels are taken as a group and permuted with the same size key. In this investigation the combination of block, bit, and pixel permutation are used respectively.
The Position Permutation Based Algorithm is use for the various techniques.

Value Transformation Based Algorithm

Values Transformation Based algorithm is based on the technique in which the value of each pixel is change to some other value. The new value of pixel is evaluated by applying some algorithm on pixel. Basically, algorithm is mathematical computation where we take input as a pixel value compute it, with some formulas and produce a new value for that pixel. Value Transformation

Based Algorithm Are Digital Signatures and Lossless Image Compression and Encryption Using
SCAN, Image Cryptosystems, Color Image Encryption Using Double Random Phase Encoding, Image Encryption Using Block-Based Transformation Algorithm and affine Transform etc.

Position- Substitution Based Algorithm

This technique is combination of both position permutation and value transformation. Position permutation and value transformation can be combined. In this technique first pixels are reordered and then a key generator is used to substitute the pixel values. The Position-Substitution Based Algorithm is use for the various techniques.

The Chaotic Encryption Process

Image Encryption

The image encryption process is shown in Figure 2. In the confusion stage of image encryption, the Bogdanov map is used to scramble (change) the pixels of the input image in a non-linear pattern. The process is repeated m times to render the image unintelligible. Let the resultant image be Cs. As the pixel positions are exchanged, the correlation among the pixels in the input image weakens. In the diffusion stage, Cs is sliced into eight bit-planes, Bi, $1 \leq i \leq 8$. These eight bit-planes are subjected to the Bogdanov map separately in such a way that the Bogdanov map is applied ni times on the bit-plane Bi. Thereafter, the scrambled bit-planes Bi are re-organized to construct the encrypted image Ce. The scrambling of the bit-planes changes the pixel value and constructs the cipher image, Ce.

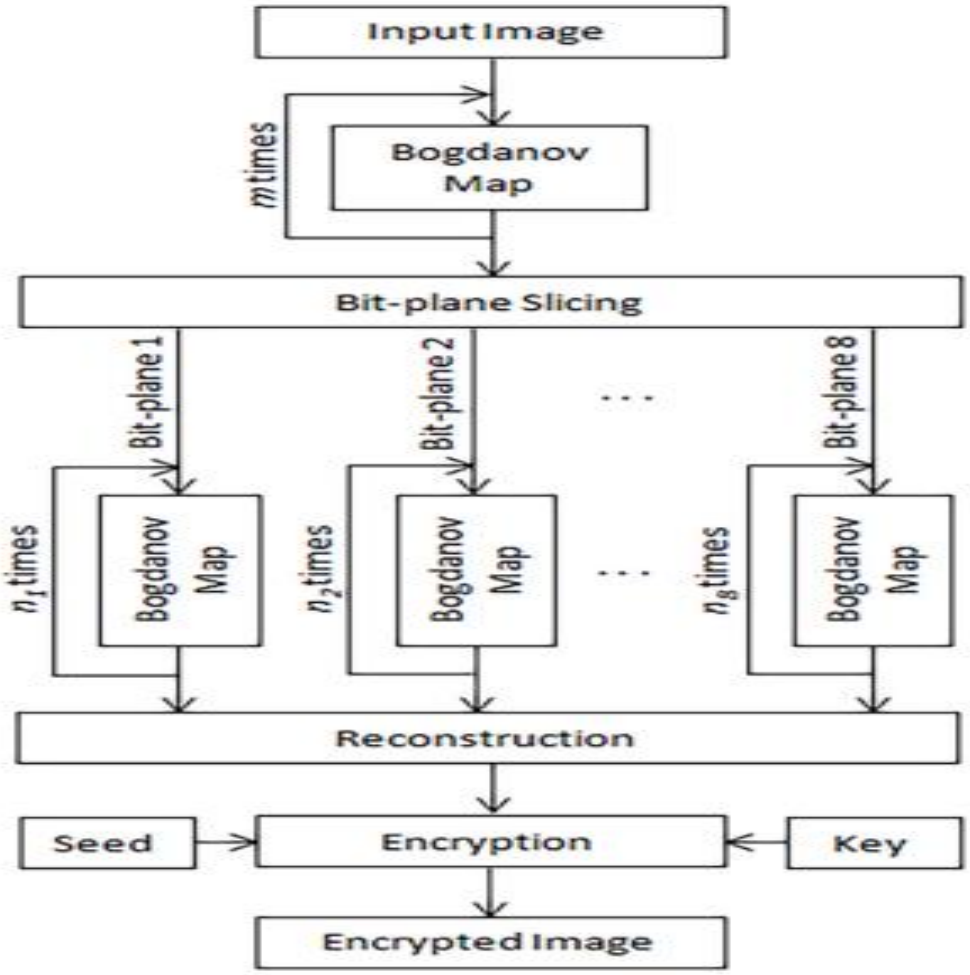


Figure 2: Image encryption process

Image Decryption

Since the proposed cryptosystem is a symmetric cipher, the decryption process is the inverse of the encryption process with the same parameter vector (m, ni , K, seed), $1 \leq i \leq 8$. The image decryption process is shown in Figure 3. First, the cipher image, C, is decrypted by using K and seed to get the partially deciphered image Ce. Ce is then separated into eight bit-planes, Bei, $1 \leq i \leq 8$, and the inverse Bogdanov map is applied ni times on the bit-plane, Bei. The unscrambled bit-planes of Bei are then re-organized to construct the scrambled image CS. The image CS is, however, unintelligible as the pixels are not positioned in their original position. The inverse Bogdanov map is once again applied m times on CS to unscramble the image. The resultant will be the original image, provided the encrypted image is not subjected to attacks.

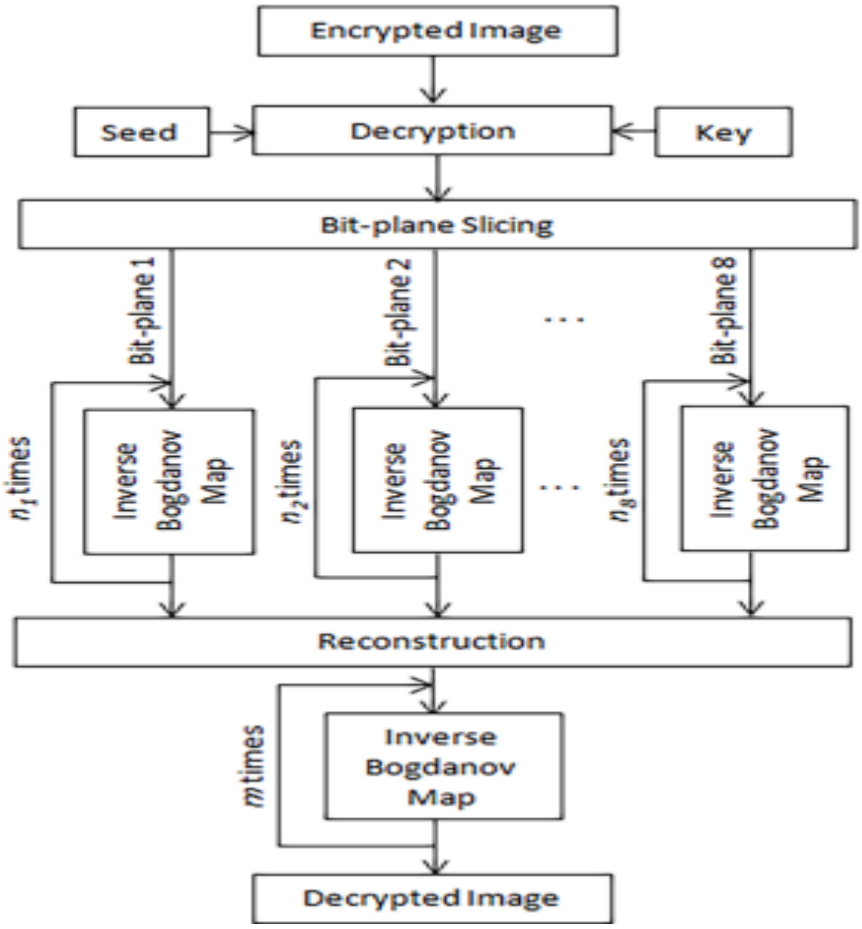


Figure 3: Image decryption process

Justification of Chaos-Based Image Encryption System

A chaos-based image encryption technique that shuffles the image's pixel locations using the Bogdanov map. The locations of the pixels are mixed up during the confusion phase. In the diffusion phase, the pixel values are changed twice: once by using a Bogdanov map to shuffle the bit-bits, planes and then by encrypting the data with keys produced by a dyadic transform. As a result, the permutation has the effects of both confusion and diffusion, and employs the Bogdanov map for permutation (shuffling).

Chaos based image encryption schemes are considered good for practical use because they have important characteristics like;

(i) They are very sensitive to initial conditions and system parameters,
(ii) they have pseudo-random property and non-periodicity as the chaotic signals are usually noise-like, etc. All these characteristics make chaos-based encryption algorithm an excellent and robust cryptosystem against any cyber-attacks.

Conclusion

A simple chaos-based image cryptosystem was implemented using the Bogdanov map to accomplish the displacement process at both pixel level and bit level. In the confusion phase, the positions of the pixels are mixed up. Its pixel values are modified twice in the diffusion phase: once by shuffling the bits of the binary plane using the Bogdanov map followed by encryption with the keys generated using the dyadic transform. It has been found that shifting pixels and gradually rearranging the image between operations works incredibly well. The additional mapping of RGB values into the image file following the remodeling of the RGB component has demonstrated the image's greater security against all currently feasible assaults. The shift and shift methodology further strengthens the operating algorithm's resistance to linear blur removal algorithms and other approaches for correcting pixel distortions in photos.

With this method, it will be challenging for any software-based blur reduction procedure to return the image to its original state. In order to accomplish these objectives, the emphasis of our next research on this subject is the use of public key cryptography in image encryption.

References

Abdeihaleem Sh, Radwan Ag & Abd-El-Hafiz Sk. (2014). "*A chess-based chaotic block cipher*". In: New Circuits and Systems Conference (NEWCAS), 12th International ed., IEEE, 405-408.

Gajendra, S. C. (2016). "*Different Image Encryption Techniques-Survey and Overview*". International Journal of Advanced Research in Computer Science and Software Engineering.

Jai, G. S., & Arun, C. (2020). "*Comparative performance analysis of chaos based image encryption techniques*". RMK College of Engineering and Technology

Lawande, Q. V., Ivan, B. R., & Dhodapkar, S. D., (2005), "*Chaos based Cryptography: A new approach to secure communications*", BARC Newsletter 258.

Robert, A. M. (1993). "*The use of genetic algorithms in cryptanalysis*." Cryptologia, vol. 17, no. 2, pp. 187–201.

Schneier, B. (1996). "*Applied cryptography. In: Protocol, algorithms and source code*". New York: Wiley.