Calculus Logarithmic Function for Image Encryption

Adil AL-Rammahi

Abstract—When we prefer to make the data secure from various attacks and fore integrity of data, we must encrypt the data before it is transmitted or stored. This paper introduces a new effective and lossless image encryption algorithm using a natural logarithmic function. The new algorithm encryps an image through a three stage process. In the first stage, a reference natural logarithmic function is generated as the foundation for the encryption image. The image numeral matrix is then analyzed to five integer numbers, and then the numbers’ positions are transformed to matrices. The advantages of this method is useful for efficiently encrypting a variety of digital images, such as binary images, gray images, and RGB images without any quality loss. The principles of the presented scheme could be applied to provide complexity and then security for a variety of data systems such as image and others.

Keywords—Linear Systems, Image Encryption, Calculus.

I. INTRODUCTION

NOW days, computers and communication technology have become widespread in domestic and official demands of our daily lives. Really, we are living in digital age representing in usages of internet, email, remote video conference, Facebook, medical reports, diagnostic of diseases, online student registration, and others. Images have taken common data via online corresponding. In other hand, important and confidential images are stored in digital ways. So, the privacy of these images must be protected from unauthorized access.


II. NEW MAIN RESULTS

This section was concerned for presenting our proposed method of encryption digital image. In our approach, the decimal logarithmic function is used in encryption stage while decimal exponent function is used in the stage of decryption. The two stages are cleared carefully as follows:

Stage 1: Encryption
1) Input original image a.
2) Compute
   \[ c = \log(a) \] .
3) Analyze
   \[ c = c_0 + c_1 + c_2 + c_3 + c_4 \] .
4) Write encrypted images \( c_0, c_1, c_2, c_3, \) and \( c_4 \).

Stage 2: Decryption
1) Input encrypted images \( c_0, c_1, c_2, c_3, \) and \( c_4 \).
2) Compute
   \[ y = c_0 + 0.1 * c_1 + 0.2 * 0.01 * c_3 + 0.001 * c_4 \] .

Adil Al-Rammahi is with the Kufa University, Faculty of Mathematics and Computer Science, Department of Mathematics, Najaf, IRQ (phone: +964(0)13391915; B.O. Box 21 Kufa, e-mail: adilm.hasan@uokufa.edu.iq).
3) Compute $b = \exp(y)$.

4) Write decrypted images $b$.

III. IMPLEMENTATIONS

For explaining the powerful of proposed method many images are tested as appearing in Table I. For explaining the goodness of proposed method, the histogram of each of the original and decrypted image implemented as showing in Table II where $h_a$ and $h_b$ represents the histograms of original image (a) and decrypted image (b) respectively.

| TABLE I |
| TEST IMAGES |
| --- | --- | --- | --- |
| Image 1 | Image 2 | Image 3 | Image 4 |
| a | c₀ | c₁ | c₂ |
| c₃ | c₄ | a | b |
In this paper, we proposed a new image encryption scheme using the decimal natural logarithmic function. For testing images as referred in Table I, we have five encrypted images ($c_0$, $c_1$, $c_2$, $c_3$, and $c_4$) corresponding to original plain image (a). These five encrypted images add more complexity for attacker and in the same way give more integrity for decryption stage. Indeed the cryptography of image has a property that the decrypted values must belong to integer numbers interval $[0,255]$. In our proposed algorithm, the allowed interval is transformed to fewer intervals under the action or calculus of logarithmic function. That’s good, but this sub interval is containing decimal numbers. Then the encrypted values over and exceed the pliable interval. And then that is considered a problem in image matrix. When we processed these errors by approximations, a deforming is resulted for encrypted image in decryption stage. So we must think in a processing procedure deals with this problem in the integer numbers field. Here we transform each encrypted value $(c)$ to five values $(c_0, c_1, c_2, c_3, and c_4)$. Each of them belongs to integer numbers interval $[0,9]$. That is leading that all encrypted images component with respect to $(c_0, c_1, c_2, c_3, and c_4)$ appears nearly black. And so, a complexity is adding against attacker, and more integrity occurs to security. The result of this method was promised. The goodness of proposed method deduces from the histogram of each the original and decrypted image as referred in Table II.

**ACKNOWLEDGEMENT**

This paper was supported by the faculty of mathematics and computer science of university of Kufa, Iraq. The author thanks all reviewers for deep reading on this paper.

**REFERENCES**


Adil AL-Rammahi was born on 1963 in Najaf, Iraq. He studied Applied Mathematics at University of Technology, Baghdad, Iraq. From the same university, he obtained his M. Sc in stability. The title of Assistant professor was awarded to him in 2002. He was awarded the degree of PhD in Fractals in 2005. He has supervised several M.Sc. dissertations. He has headed the Mathematics Department for three years from 2008-2011. His area of research is Fractals, Numerical Analysis, Cryptography and Image Processing. He published more than 25 papers and one book. He was selected as an editor, reviewer and a scientific committee member in many journals and conferences.