A Robust Image Encryption Scheme Using Multilevel Cryptographic Algorithms

Dr. Elena Petrova, Dr. Dmitry Sokolov, Dr. Anastasia Ivanova
Department of Physics, Lomonosov Moscow State University, Moscow, Russia
Institute of Applied Mathematics, Russian Academy of Sciences, Moscow, Russia
Faculty of Computational Sciences, Saint Petersburg State University, Saint Petersburg, Russia

ABSTRACT

Encryption is a common technique to uphold image security. With the ever increasing growth of multimedia applications, security is an important issue in communication and storage of images encryption is one of the ways to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand, to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. In this paper an advanced multilevel based encryption technique is used to encrypt the images. When intruders try to access the image content it will be more complex for double encryption. That is the strength of this proposed method.

***Keywords**: Image Encryption, Cryptography, Security, Multilevel Encryption.*

I. INTRODUCTION

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in different processes. Therefore, the security of image data from unauthorized uses is important [1]. Image encryption plays an important role in the field of image hiding. Image hiding or encrypting method and algorithm can be very from simple methods to more complicated and reliable frequency method [2]. Basically Image Encryption means that, convert the image into unreadable format. Multimedia systems mostly base security on a restricted access to services. In the context of real-time imaging applications, this model suffers several drawbacks [3]. Applications become vulnerable to password attacks and once exposed attackers have access to all the data. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc [9].

Types of image encryption schemes
Schemes can be classified into three major types:

- Position permutation,
- Value transformation and
- Visual transformation.

Four types of images
Binary images
A **binary image** is a digital image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white though any two colors can be used. The color used for the object(s) in the image is the foreground color while the rest of the image is the background color. Binary images are also called *bi-level* or *two-level* [4]. This means that each pixel is stored as a single bit (0 or 1). The names *black-and-white*, *B&W*, monochrome or monochromatic are often used for this concept, but may also designate any images that have only one sample per pixel, such as grayscale images [8].

Grayscale image
Many image processing algorithms are defined for grayscale (or else monochromatic) images. Extend the data storage type defined on this page to support grayscale images [5]. Define two operations, one to convert a color image to a grayscale image and one for the backward conversion. To get luminance of a color use the formula recommended by CIE:
$L = 0.2126 \cdot R + 0.7152 \cdot G + 0.0722 \cdot B$

Indexed Images

In imaging, indexed color is the term used to describe reduced color mapping of 8-bit or less. This is done to reduce images to their smallest size and these images are most commonly used on Web pages as they are small and quick to load [6]. The 256 color palette is mapped for best results on the Internet, taking into account the differences between the Windows and Macintosh color palettes [7].

True Color Images

True color may refer to:

- **True-color**, the rendition of an object's natural colors through an image.
- **True Color**, the use of a 24-bit color depth to display an RGB image.
- **Color of water** (**true color**), a scale used to determine the color of water after all suspended material has been filtered out [7].

II. PROPOSED METHODOLOGY

Encryption Algorithm steps:

Step 1: Select an image
Step2: Split the image into pixels
Step3: Get image RGB colors on each pixels based on alpha color.
Step4: Add key value to pixels
Step5: Add position of the pixels selecting Row wise
Step 5: Apply the given formula for substitution

$$E = (p + k + i) \% 256$$

p – Pixel value, k – key, i – Position.
Step 6: Apply the transposition
Step 7: Create the image using encrypted pixels

Decryption Algorithm steps:

Step 1: Get the encrypted image
Step 2: Here the same encryption key is used
Step 3: To assign the position of the pixels
Step 4: Apply the transposition
Step 5: To apply the formula

$$D = ((E – k – i) + 256) \% 256$$

E – Encrypted image, k – key, i – Position.
Step 6: Get image RGB colors
Step 7: Retrieve the original image

Characteristic of Proposed Method

Simplicity: Proposed algorithm is very simple. Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.
Security: Due to the length of the key proposed technique is very much secured.
Flexibility: The flexibility issues of proposed encryption technique are very high which is referring to the use of keys and whether the key lengths are set, or whether different key lengths can be used.

III. RESULTS AND DISCUSSIONS

- Browse an image
- Click the grayscale button the color image converted into grayscale image
- The grayscale image was displayed

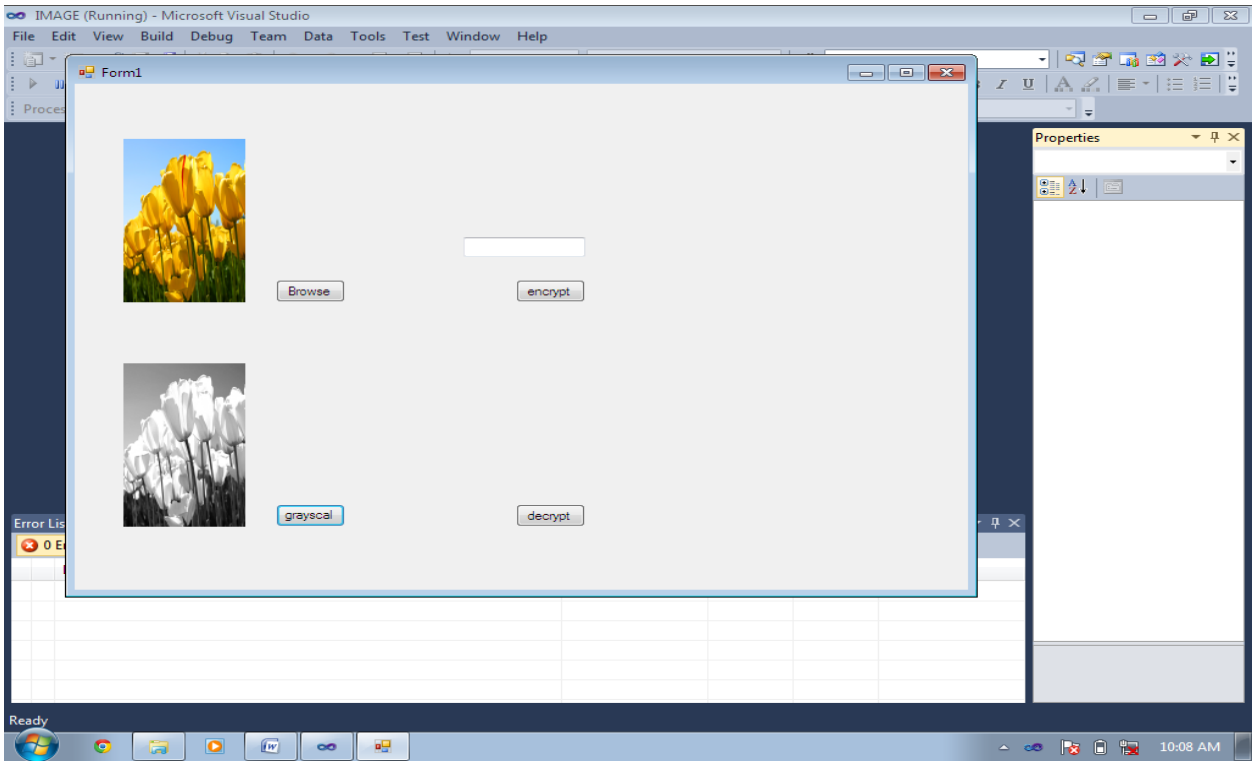

Figure 1. Grayscale Image

Encryption

- Click to encryption button
- The multilevel encryption algorithm transposition and substitution will be performed, when we enter the encryption key value.
- Finally the encrypt image displayed.

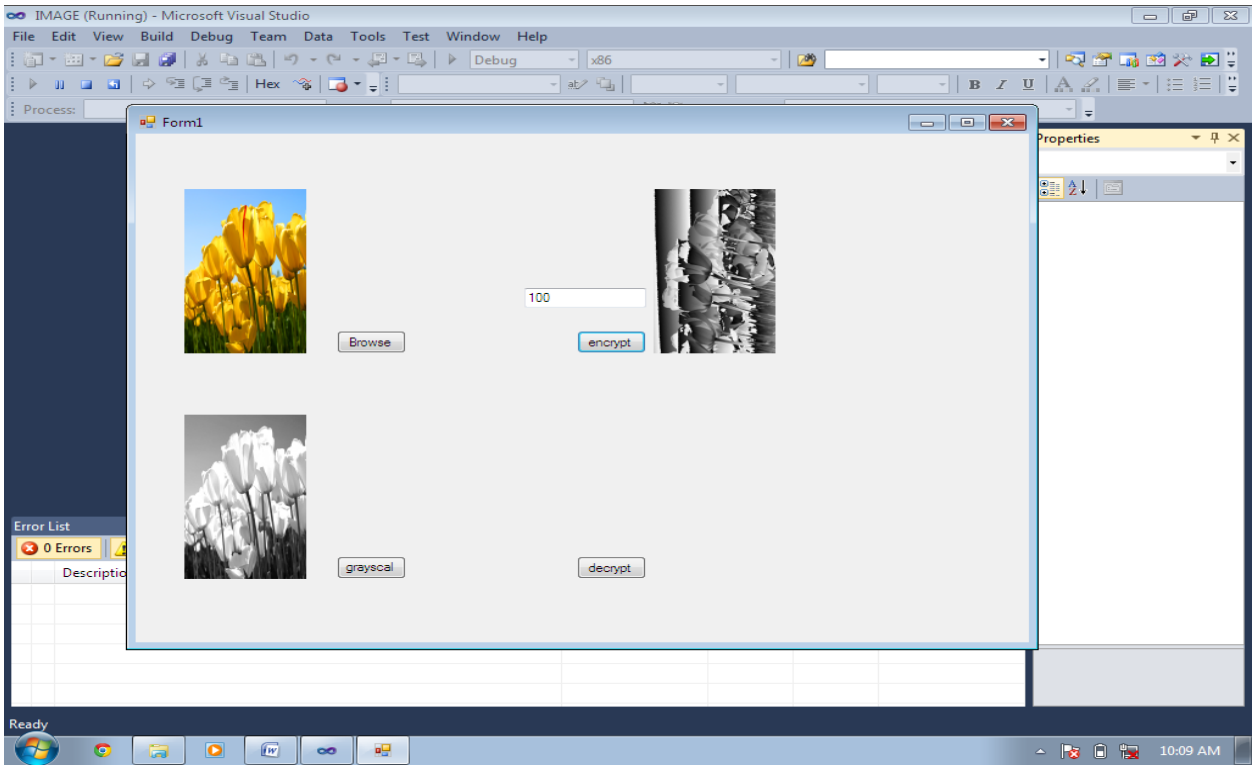

Figure 2. Encrypted Image

Decryption

Decryption is the reverse process of the image encryption.

- When we enter the decrypt button the image will be displayed at grayscale level.

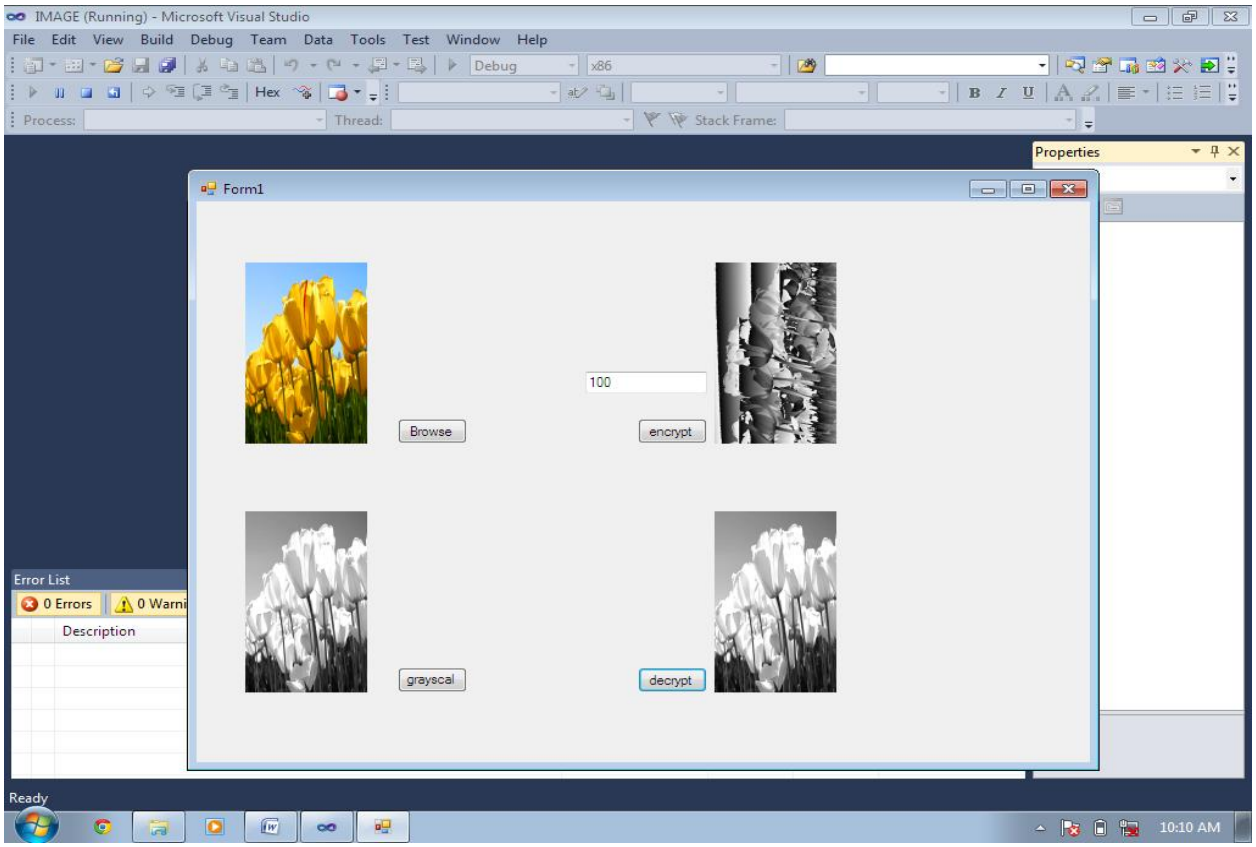

Figure 2. Decrypted Image

IV. CONCLUSION

In this paper a simple and strong mechanism has been proposed for image security using a combination of multilevel encryption based image transformation and proposed encryption techniques. There are so many different techniques should be used to protect confidential image data from unauthorized access. But this proposed method processing the combination of both transposition and substitution algorithm. When the unauthorized parties try to access the original image content it will be more complex for this proposed multilevel encryption method. That is the main strength and security consideration of this proposed method.

REFERENCE

1. *Dr. A. Padmapriya and P. Subhasri, "Cloud Computing: Security Challenges & Encryption Practices", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), March 2013 Volume 3, Issue 3, ISSN: 2277 128X, pp. 255- 259.*
2. *P. Subhasri and Dr. A. Padmapriya, "An Implementation of Reverse Caesar cipher (RCC) Algorithm in Google Cloud using Cloud SQL", International Journal of Computer Trends and Technology (IJCTT), July 2013 Volume 4, Issue 7, and ISSN: 2231 - 2803, pp. 2257 – 2262.*
3. *P.Subhasri and Dr. A. Padmapriya, " Enhancing the Security Of Dicom Content Using Modified Vigenere Cipher", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.55, May 2015, pp. 1951-1956.*
4. *P. Subhasri and Dr. A. Padmapriya, "Multilevel Encryption for Ensuring Public Cloud", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) in July 2013, Volume 3, Issue 6, ISSN: 2277 128X. pp. 527-532.*
5. *P. Subhasri and Dr. A. Padmapriya, "Ensuring Security Of Dicom Content Using Transposition Based AES", National Conference NCDS-2014 in S. T. Hindu College, Nagerkovil in August 2014.*
6. *Rolf O, "Contemporary Cryptography", Architect House, Boston, London, 2005.*
7. *Britt.P, "Tightening Security", Information Today, Retrieved March-2007.*

8. *Andrew S. Tanenbaum, Networks Computer, 5th edition, Pearson Education, ISBN-10: 0132553171.*
9. *Adam Berent, "Advanced Encryption Standard by Example", ABI Software Development, Vo1.7.*