iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8024

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

A Novel Approach for Image Encryption and Decryption

Yogesh Kumar[1], Mamta Sohal[2]
[1,2]*Department of Computer Science South Point Institute of Technology & Management (SITM), Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat*

Abstract*: *The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, and this method is called encryption. To make a message unintelligible, it scrambled according to a particular algorithm, which is agreed upon beforehand between the sender and the intended recipient. Then, recipient can reverse the scrambling protocol and make the message comprehensible. This reversal or scrambling is known as decryption. The advantage of using encryption and decryption is that, without knowing the scrambling protocol, the message is difficult to recreate. Cryptography has its roots in communication security. Security of data becomes more important when we transfer data over insecure communication medium. Data transfer refers to moving data from source location to destination location. To have a secure data transfer, few method can be applied, and one of them is encryption of data, prepare it to be transferred in encrypted way and decrypted when the data want to be used. In this work we provide a novel approach with unique key method for performing the task of encryption and decryption on the digital image.

Keywords*: *Symmetric key Cryptography, Asymmetric key Cryptography, Communication Security

I. INTRODUCTION

Information that can be read and implicit without any special procedures or method is termed as plaintext or clear text. The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, and this method is called encryption. To make a message unintelligible, it scrambled according to a particular algorithm, which is agreed upon beforehand between the sender and the intended recipient. Then, recipient can reverse the scrambling protocol and make the message comprehensible. This reversal or scrambling is known as decryption. The advantage of using encryption and decryption is that, without knowing the scrambling protocol, the message is difficult to recreate. Cryptography has its roots in communication security.

The antagonist is an intruder who has full control over this channel, being able to read their messages, delete messages and insert messages. The two entities A and B trust each other. They want a protection from the intruder. With the help of cryptography we can securely transfer data from one point to another over insecure network communication. Encryption is the formal name for scrambling program. The normal data, unscrambled, called plaintext or clear text and transform them so that unintelligible to the outside observer, the transformed data is called enciphered text or cipher text [1].

The science of consuming the calculation and math behind the procedure to encrypt and decrypt data is called cryptography. Cryptography facilitates to accumulate the sensitive information or pass on it through the insecure networks in order to keep it unreadable from public except the intend receiver.

Figure 1 below shows the general concept of cryptography.

Figure 1: Encryption and Decryption

Although cryptography is the skill or art of securing data, the skill of analyzing and breaking secure communication is considered as cryptanalysis. Classical cryptanalysis implicates a fascinating arrangement of application of mathematical tools, analytical reasoning, tolerance, pattern finding, willpower, and good fortune. Cryptology comprises of both cryptography and cryptanalysis [2].

In this work we provide a novel approach with unique key method for performing the task of encryption and decryption on the digital image.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

II. OVERVIEW OF WORK

To make a message unintelligible, it scrambled according to a particular algorithm, which is agreed upon beforehand between the sender and the intended recipient. Thud, recipient can reverse the scrambling protocol and make the message comprehensible. This reversal or scrambling is known as decryption. The advantage of using encryption and decryption is that, without knowing the scrambling protocol, the message is difficult to recreate. Cryptography has its roots in communication security.
Communication security [3] is described in this figure 2 below.

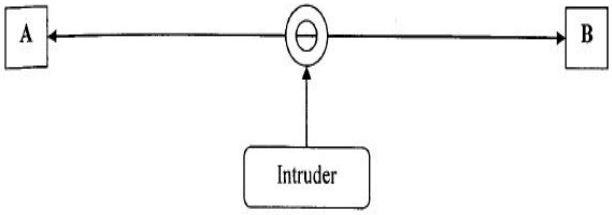


Figure 2: The Communication Security

The above figure is the description of two entities that tries to communicate over an insecure channel. The antagonist is an intruder who has full control over this channel, being able to read their messages, delete messages and insert messages. The two entities A and B trust each other. They want a protection from the intruder. Cryptography gives them the means to construct a secure logical channel over an insecure physical connection.
Encryption is the formal name for scrambling program. The normal data, unscrambled, called plaintext or clear text and transform them so that unintelligible to the outside observer, the transformed data is called enciphered text or cipher text. Using encryption security professional can virtually nullify the value of an interception and the possibilities of effective modification and fabrication.
Encryption is clearly addressing the need for confidentially of data. Additionally, it can used to ensure integrity that the data cannot be read and cannot be easily changed in the meaningful manner. It is basis of the protocol that enables to provide security while accomplishing an important system or network task. A protocol is an agreed-on sequence of actions that leads to desirable results. For example, some operating system protocols ensure availability of resources as different tasks and users request them.
Thus, encryption can also be thought of as supporting availability. That is, encryption is at the heart of methods for ensuring all aspects of computer security [4].
The two main elements in the encryption process are the keys and the algorithms. The algorithms are defined as complex formulas that dictate the rules of how the plaintext will be encrypted to cipher text. Keys are likely the strings of random bits that are used by the algorithms. In some of the encryption technologies, if two end-points need to communicate with one another, by using encrypted data, they have to use the same algorithm, and most of the time, the same key. In some different encryption technologies, they must use different but related keys for this algorithm [5].
Cryptography algorithms are either asymmetric algorithms, which use asymmetric keys or symmetric algorithms, which use symmetric keys.

A. Symmetric Key Encryption

In symmetric key encryption, the receiver and the sender use the same key for decryption and encryption. Symmetric key encryption is also called a secret key, because both sender and receiver must keep the key secret and protected. If two users want to exchange data using secret key encryption, both of them must acquire a copy of the same key [6][7].

B. Asymmetric Key Encryption

Asymmetric key algorithm is also known by the public key algorithm. Public key cryptography described a two-key cryptosystem in which two parties could communicate securely over a non-secure communication channel without having to share a secret key. They worked out the problem of the secret key distribution by using two keys instead of a single key. A public key, which can be known by everyone, and a private key, which should be kept secret and known only by the owner.

III. PROPOSED WORK

Cryptography [8] is playing a major role in data protection in applications running in a network environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity

of the sender. It has become more critical to our day-to-day life because thousands of people interact electronically every day; through e-mail, e-commerce, ATM machines, cellular phones, etc. This geometric increase of information transmitted electronically has made increased reliance on cryptography and authentication by users.

There are many ways of classifying data cryptographic algorithms – Secret Key Cryptography, Public Key Cryptography and Hash function. In this work we will use secret key cryptography (SKC).

The SKC method uses only a single key for both encryption and decryption. The schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing while block cipher scheme encrypts one block of data at a time using the same key on each block.

Encryption and decryption attain by single key is the finest technique of image security. Single key assigned for image encryption and it is encoded. Then the key is send via secure way for decryption purpose. Subsequently the key is safely received and apply decryption process and obtain original image. The proposed method block diagram is shown in figure 3 below.

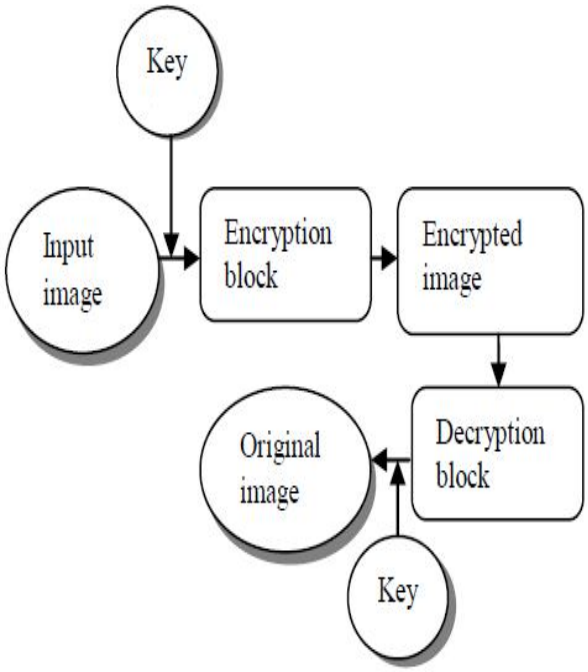


Figure 3: Proposed Work

The encrypt part is used to conceal the information of image. Thereafter no individual can perceive the information. Decrypt part is utilized the secret information to unlock and lay up as original image.

IV. IMPLEMENTATION RESULT

Figure 4 below shows the main GUI screen of our implementation of Image encryption and decryption.

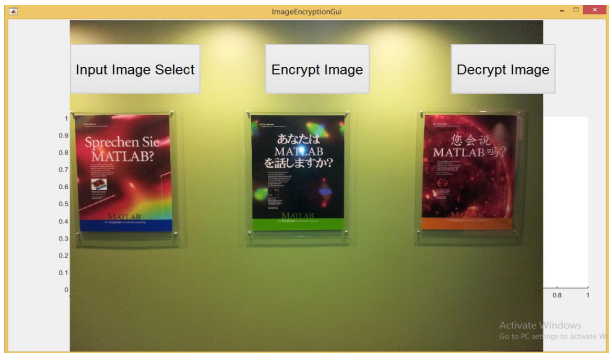


Figure 4: The main GUI screen of our implementation

Figure 5 below shows the input image selected for encryption.

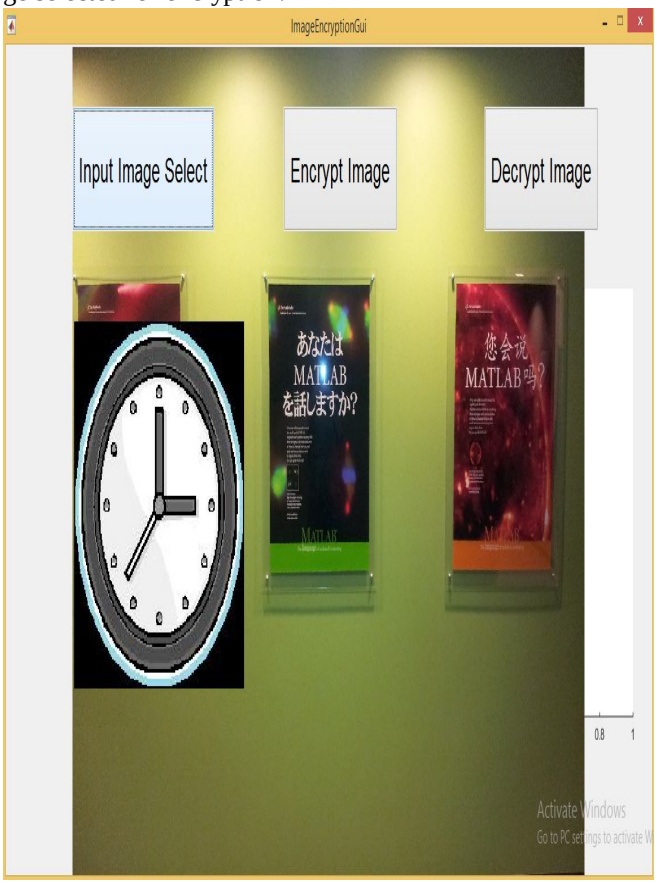


Figure 5: The input image selected for encryption.

Figure 6 below shows the encrypted image after applying unique key and image encryption algorithm.

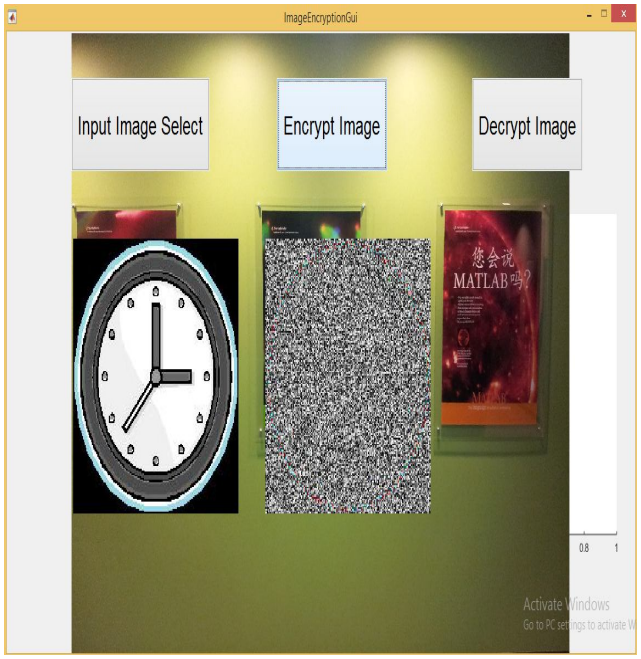


Figure 6: The encrypted image of original image using image encryption algo & key.

Figure 7 below shows the decrypted image after aplying inverse image processing functionality with image decryption key.

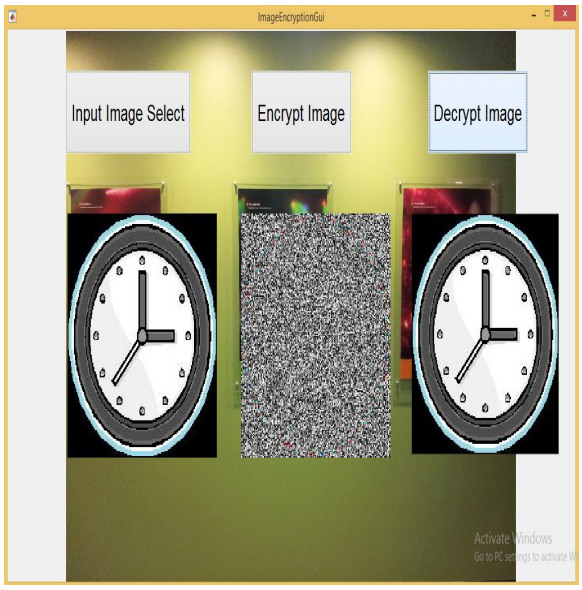


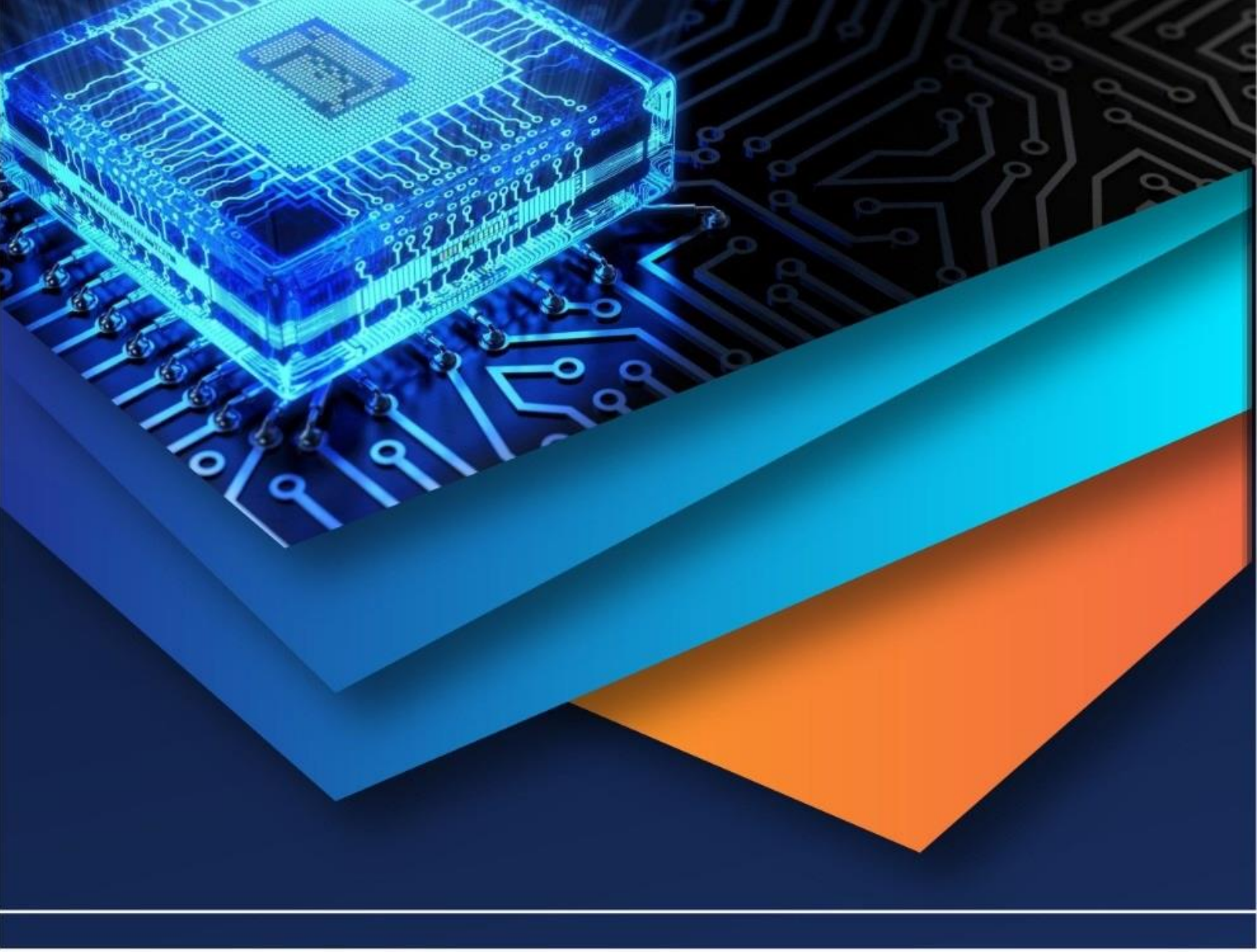
Figure 7: The image after decryption with image decryption key

V. CONCLUSION

Cryptography has its roots in communication security. Security of data becomes more important when we transfer data over insecure communication medium. Data transfer refers to moving data from source location to destination location. To have a secure data transfer, few method can be applied, and one of them is encryption of data, prepare it to be transferred in encrypted way and decrypted when the data want to be used. In this work we provide a novel approach with unique key method for performing the task of encryption and decryption on the digital image.

REFERENCES

[1] Nentawe Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment", International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013.
[2] Stallings, W. (1999). "Cryptography and Network Security". Upper Saddle River, N.J.: Prentice Hall.
[3] Swapnil G. Deshpande, Pradeep. B. Dahikar, (2011), "Strengthening of Data Security Against Its Attack", Int. J. Advanced Networking and Applications, Vol.3, pp. 29-35.
[4] T Bhaskara; Yaragunti, Hema Suresh; Reddy, T Sri Harish; Kiran, S.(2013), "An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique", International Journal of Computer Technology, 4.6883-891.
[5] Xie, R, Wang, M., & Hai, B. (2015), "Image Encryption Research Based on Key Extracted from Iris Feature", IJSIA, 9(6), 157-166.
[6] Ayushi, M. (2010), "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, 1(15), 1-6. http://dx.doi.org/10.5120/331-502.
[7] Mohamed Abomhara, Omar Zakaria, Hamdan O. Alanazi, (2010). "Suitability of Using Symmetric Key to Secure Multimedia Data", Journal of Applied Sciences,165-166.
[8] Diffie, W. M.E. Hellman, (1976), "New Directions in Cryptography", IEEE Trans. Inform. Theory, 22: 644-654.
[9] Rabah, K., (2005). "Theory and Implementation of Data Encryption Standard, A Review", Inform. Technol. J., 4: 307-325.
[10] Jessie-Lee Nichols, "How and When To Use Different Types of Image Files", November 15, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY