Enhanced Polygram Substitution Algorithm For Image Security

Dr. S. Kiran[1], Mr. B. Lakshmi Narayana Reddy[2], Mr. B. Siva Vishnu Mohan Reddy[3],
Dr. T Bhaskara Reddy[4]

1 Assistant Professor in the department of Computer Science and Engineering, YV University College of Enginnering., Proddatur
2 Scholar in the department of Computer Applications YV University., Kadapa
3 Assistant Professor in the department of Computer Science and Engineering, Sri Venkateswara Institute of Science and Technology. Kadapa
4 Associate Professor, Department of Computer Science and Technology, S K University, Anantapur.

Abstract

Now-a-days securing the privacy of data is becoming more prominent. In the past decade the security and integrity of data or multimedia data is main concern. In the present scenario the data transferred over computer networks more vulnerable. The growth of networked multimedia systems has created a need for the security of images when images are transmitted across public networks. Government, military, financial institutions, hospitals and private business deals with confidential images. Protecting confidential images is an ethical and legal requirement. The protection of image avoids all possible threats from the exploiters is a challenging task. Image transfer can be successfully transmitted if no one shares this secret information with others. This paper summarizes and presents an approach to image integrity and security in addition to conventional network security protection and analyses the security of image with enhanced speed of encryption and decryption. This process uses cipher formation via Polygram substitution cipher technique with some modification. This cipher used by various cryptographic algorithms thus making the computer process a lot faster and secure.

1. Introduction

Cryptography[4,5] defined as "the science and study secret writing", the way in which data can be encoded to prevent disclosure of their contents through eavesdropping or message interception[3] and other methods, so that only certain people can see the real data. The ability to protect and secure data[3] is vital to growth of electronic data and to the growth of the Internet itself. With regards to confidentiality [1], cryptography is used to encrypt data residing on storage devices or travelling through communication channels[3,5] to ensure that any illegal access is not successful. Also cryptography is used to secure the process of authenticating different parties attempting any function on the system. Cryptography problem can be broken down into five requirements that must be addressed:

1. Confidentiality: Assuring that preventing disclosure of sensitive information.
2. Authentication: Assuring the identity of legitimate users.
3. Authorization: Assuring that a certain party allowed performing an operation.
4. Data Integrity: Assuring that the data is not modified illegally.
5. Non-Repudiation: Assuring that someone cannot deny something.

Confidentiality can be achieved by cryptography encryption; authorization can be achieved by providing credentials such as passwords, smart cards…etc. Data integrity and Non-repudiation can be achieved by means of Digital signatures[10].

2. History

Cryptography began thousands of years ago. The very word cryptography comes from the Greek

words Kryptos and Graphein, which means hidden and writing respectively. Cryptography was already used in ancient times in private and military communications.
The art science of cryptography showed no major changes or advancements until middle Ages. Encryption in modern times is achieved by using algorithms that have a key to encrypt and decrypt information. Beginning around the 1990s, the use of the Internet for commercial purposes and the introduction of e-commerce called for a widespread standard for encryption.

3. Initial Discoveries and Research Objectives

The main difficulty with cryptography is distributing secret keys[2] over a secure channel. To distribute secret keys to each user pair becomes very expensive. Many cryptographic schemes consist of pairs of operations, such as encryption and decryption, or signing and verification. In a well-designed cryptographic scheme, the security of the scheme depends only on the security of the keys used. Even if antagonist know the what algorithm is used, they cannot gain access to the data unless they also have the proper key.

The confidentiality, Authentication, Authorization, Integrity, and Non-repudiation are of great importance in providing security. Failure in any of these areas can result in disruption to the security services.

The Objectives are achieved through the implementation of security policies:

1. Ensure that information is accessible only to those authorized to have access.
2. Safeguard the accuracy and completeness of information and processing methods.
3. Ensure that information it manages shall be secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.
4. Meet all security requirements under appropriate regulations, legislation, organization policies and contractual obligations.
5. Address the security of all services and processes to ensure that risks are identified and appropriate technologies are implemented and documented.

4. Polygram Substitution Method

Polygram substitution technique[1] replaces one block of plain text with a block of cipher text – it does not work on a character-by-character basis. For instance, HELLO could be replaced by YUQQW, but HELL could be replaced by a totally different cipher text block TEUI. These cryptosystems make crypt analysis harder by destroying single character frequencies, preserved under simple substitution ciphers.

5. Application of Polygram Substitution Method for Images

In general Polygram substitution method applied for block of characters. In this paper this substitution applied for image pixel intensities[7,9]. The following are the problems with Polygram substitution method:

1. Different keys are required for each encryption or decryption.
2. For each repeated same block of input produces different output that increases encryption time.
3. Occupies more storage space for each encoded data.
4. One block replaced by another block with specific range of values makes ease for intruders to identify values.

6. Solution for Polygram Substitution Method for Images

1. First reverse all image pixel intensity values before applying Polygram substitution method.
2. Then adding different keys for each pixel intensity value as in the same way as Polygram substitution method does.
3. For repeated pixel intensities also same procedure applicable.
4. As the pixel intensity values are used for both encryption and decryption so it is not easily rectified by the intruder[1,2].

5. Adding and subtracting the consecutive numbers from each intensity value increases the security and it is not easily compromised.

7. Enhanced Polygram Substitution Procedure for Images

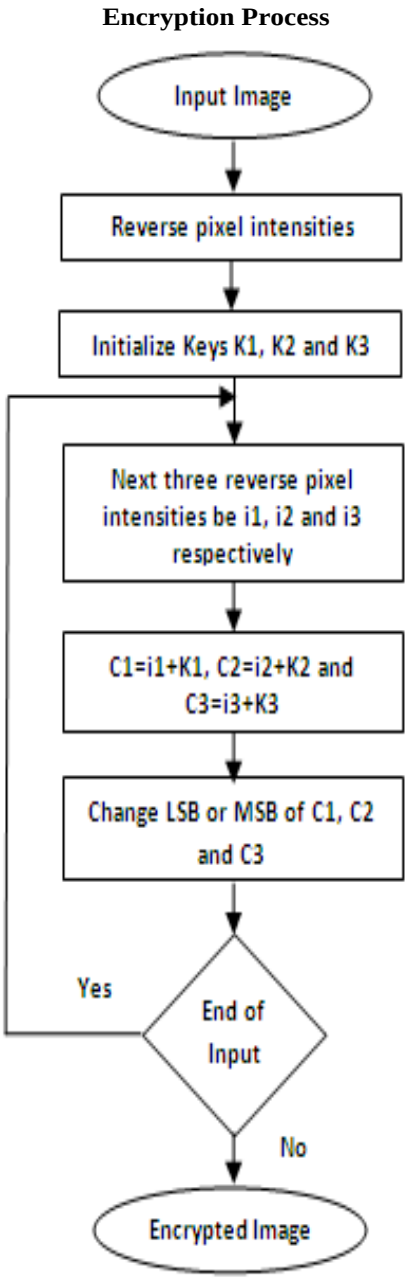

Figure 1: Proposed Image Encryption Process

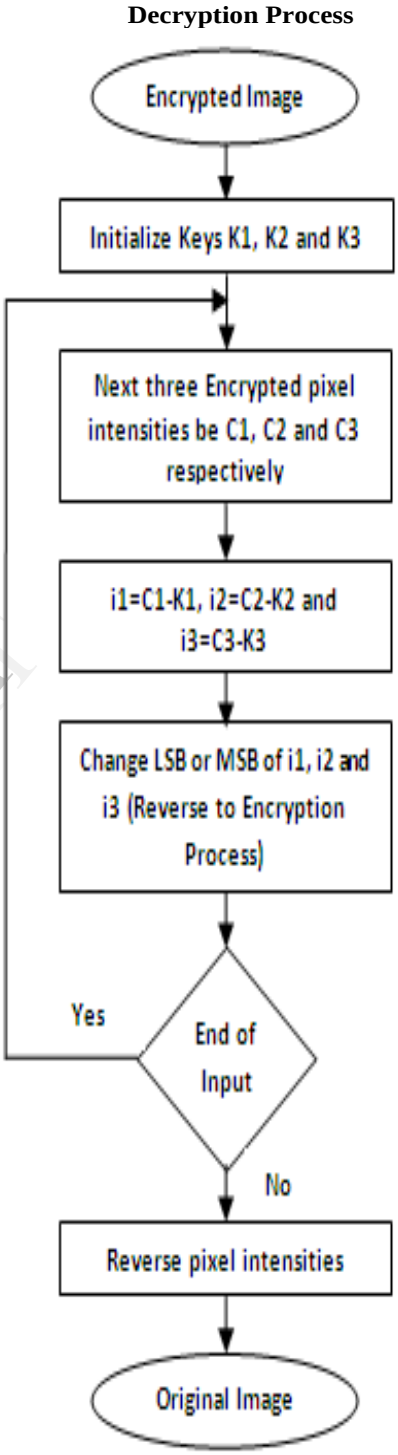

Figure 2: Proposed Image Decryption Process

8. Experimental Results

The proposed work implemented in C language. We take a gray-scale "baboo" image of 50x50 size for experimental purposes. The original image and its histogram shown in figure 3(a)-(b). The reversed image and its histogram shown in figure 4(a)-(b). The encrypted image and its histogram shown in figure 5(a)-(b). The LSB or MSB modified encrypted image and its histogram shown in figure 6(a)-(b). The distribution of gray values of encrypted image has good distribution property. Hence, the encrypted image does not provide any information regarding the distribution of gray values to opponent.

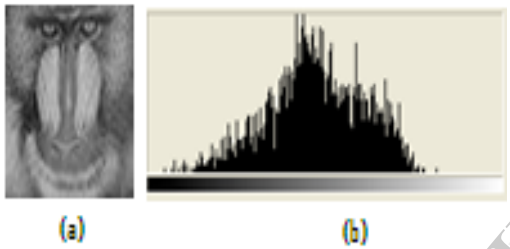

Figure 3: (a) Plain image; (b) Plain image histogram

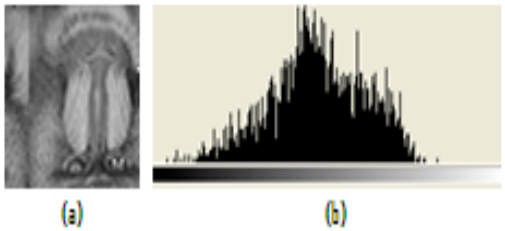

Figure 4: (a) Reversed image; (b) Reverse image histogram

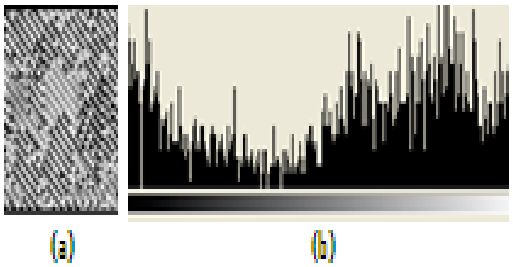

Figure 5: (a) Encrypted Image; (b) Encrypted image histogram

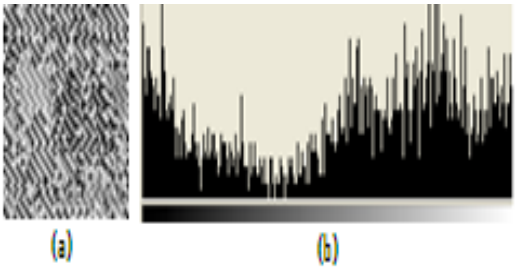

Figure 6:(a) LSB or MSB modified image; (b) LSB or MSB modified image histogram

9. Conclusion

In this paper a simple and strong method has been proposed for image security using a combination of transposition, encryption, and LSB or MSB modification technique. Both Colour and Black and White images of any size saved in raw format can be Encrypted and Decrypted. In this paper a new modified PolyGram substitution technique has been proposed. Detailed analysis has shown that new scheme offers high security. As we can see from the experimental results gray values distributed has good property that hides image gray levels in secure manner. We used three layers of security to secure image. First reverse image, Image encryption with key, and LSB or MSB modification.

10. References

[1] Refined Polygram Substitution Cipher Method: A Enhanced Tool for Security , Ekta Agrawal, Dr. Parashuram Pal, International Journal of Engineering and Innovative Technology(IJEIT) Volume 2, Issue 1, July 2012.

[2] Nalani N, G. Raghavendra Rao,' Cryptanalysis of Simplified Data Encryption Standard via Optimisation Heuristics; IJCSNS, Vol.6 No.1B, January 2006.

[3] A K Verma, Mauyank Dave and R.C Joshi, 'Genetic Algorithm and Tabu Search Attack on the Mono Alphabetic Substitution Cipher in Adhoc Networks; Journal of Computer Science 3(3): 134-137, 2007.

[4] Atul Kahate, "Cryptography and Network Security", 2nd Edition, Tata Mc-Grew – hill Publisher ltd, 2011.

[5] William Stallings," Cryptography and Network Security: Principles and Practice", 2/3e Prentice hall, 1999.

[6] Jagadish H. Pujar, Lohit M. Kadlaskar (2010) "Anew lossless method of image compression and decompression using Huffman coding techniques" Journal of Theoretical and Applied Information Technology

[7] Rafael C.Gonzalez,Richard E.Woods "Digital Image Processing "Second edition Pearson Education,Printice Hall

[8] G.C Chang Y.D Lin (2010) "An Efficient Lossless ECG Compression Method Using Delta Coding and Optimal Selective Huffman Coding" IFMBE proceedings 2010, Volume 31, Part 6, 1327-1330, DOI: 10.1007/978-3-642-14515-5_338.

[9] The Scientist and Engineer's Guide to Digital Signal Processing by Steven W. Smith.Ph.D

[10] R. Pagh and F. F. Rodler, Cuckoo Hashing, in 9th Annual European Symposium on Algorithms, v.2161 of Lecture Notes in Computer Science, pp. 121-133, Springer-Verlag, 2001.

AUTHORS PROFILE

Dr.S.Kiran is an Assistant Professor in the department of Computer Science and Engineering at Yogivenama University , Kadapa, A.P. He has completed his M.Sc and Ph.D in computer science from S.K.University. He has acquired M.Tech from Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 5 years. He has published 4 National and International publications.. His research interests are in the field of image Processing, computer networks, data mining and data ware house. E-Mail:rkirans125@gmail.com

Mr. B. Lakshmi Narayana Reddy is Research Scholar in the department of Computer Science at Yogi Vemana University, Kadapa, A.P. He acquired M.Sc in Computer Science from S.V.University, Tirupathi and M.E.(CSE) from Sathyabama University, Chennai. E-Mail: boreddynarayana @gmail.com

Mr. B. Siva Vishnu Mohan Reddy is an Assistant Professor in the Department of Computer Science and Engineering at Sri Venkateswara Institute of Science and Technology, Kadapa, A.P. He has completed his B.Tech (CSE) from Gulburga University and M.Tech (CSE) from Visweswaraiah University, Karnataka. E-Mail:sivvishnu @gmail. com

Dr.T.Bhaskara Reddy is an Associate Professor in the department of Computer Science and Technology at S.K. University, Anantapur A.P. He holds the post of Deputy Director of Distance education at S.K.University and He also the CSE Cocoordinator of Engineering at S.K. University. He has completed his M.Sc and Ph.D in computer science from S.K.University. He has acquired M.Tech from Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 17 years. He has published 47 National and International publications. He has completed major research project (UGC). Four Ph.D and Three M.Phil have been awarded under his guidance. His research interest are in the field of image Processing, computer networks, data mining and data ware house. E-Mail:bhaskarreddy _sku@yahoo.co.in