International Journal of Modern Trends in Engineering And Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Image Encryption and Decryption Using Different Algorithm

Prajkta Powar[1], Prof. M.M.Mukhedkar[2]

[1] *Department of E & TC Engineering, D Y Patil College of Engineering, Pune, powarprajkta@gmail.com*
[2] *Department of E & TC Engineering, D Y Patil College of Engineering, Pune, moresh.mukhedkar@gmail.com*

Abstract — This paper focuses mainly on the different kinds of image encryption and decryption techniques. In addition focuses on image encryption techniques, As the use digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. There are various techniques which are discovered from time to time to encrypt the images to make images more secure. This papers dealing with image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image. In this paper a Survey of Different Image Encryption and encryption techniques that are existing is given. It additionally focuses on the functionality of Image encryption and decryption techniques.

Keywords- Block-Based Transformation Algorithm, Blowfish Algorithm, Image encryption, Image decryption Security, Selective encryption algorithm.

I.INTRODUCTION

In today's world, communication play important role communication is the process which can transmit data one location to another location. During this communication, security is important issues. Internet is one of communication media are used to information exchanges like digital images, text, video and the storage of data in open networks, in which illegal users can obtain the important information. So Encryption algorithms have been used to provide security. In encryption, unauthorized user cannot access the data only authorized person having the key can obtain the original data.

The various image encryption techniques can be classified into three major categories: transposition techniques (position permutation), substitution techniques (value transformation) and the combination i.e. transposition-substitution technique. The transposition techniques used to

shuffle the pixel position within the image itself and usually have low security because histogram of the shuffled image remains same substitution techniques, they modify pixel value of the original image and have the potential of low computational complexity and low hardware cost. transposition-substitution technique, combination both position permutation and value transformation and has the potential of high security. Another technique for securing digital images is based on the use of chaotic functions.

Section II gives a basic concept about the current image encryption schemes. In Section III, Selective encryption algorithm. Section IV Block-Based Transformation algorithm and section V Blowfish algorithm section VI Result of image encryption section VII conclusion of the paper.

II.BASIC CONCEPT

In real time application for secure image transmission over internet and through wireless networks more number of techniques are used. Technique like cryptography, Visual Cryptography, stenography, watermarking .this all are encryption technique.
Image encryption algorithm used 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 the content without a key for decryption. Encryption is process of encoding plain text data into cipher text data is called encryption and the reverse process of transforming cipher text data to plain text data is called as decryption. As shown in fig[1].

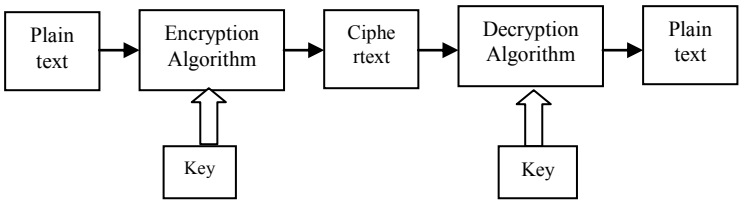

Fig 1: Baisc Encryption/Decryption Blocked Diagram

III. LITERATURE REVIEW

[7]In this paper, selective encryption algorithm is used to divide the image into regions of fixed size. These regions act as units for processing the image. Selective Encryption encrypt only a part of the image remaining part of the image unaltered. Here, only region are considered for encryption. Selective Reconstruction algorithm deals with decrypting only a part of the encrypted image. Both the methods give a fair amount of reduction in the encryption time. Once the segmentation and permutation of regions is completed, the regions are encrypted independently.
[5] In this paper, an image encryption method is proposed by using the linear mixing model of blind source separation *(BSS).* encrypt multiple images with the same size by mixing them with the same number of statistically independent key images, the size of which is equal to that of the images to be encrypted. Since these multiple images cover mutually through mixing among them while the key images cover them, and there is not any restriction on the key space, the proposed method has high level of security.
[11]In this paper, a novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data hiding key, or obtain an image similar to the original one using only the encryption key.
[15]In this paper, we have studied the problem of condentiality preserving content-based image search. This problem has many practical applications such as secure online services that help manage personal image collections, and the problem also has several challenging

research issues, such as achieving a good trade-off between security and efficiency for practical applications that demands high efficiency and least user involvement. We have reviewed two major types of techniques for this problem, namely techniques based on homomorphic encryption, and techniques based on visual feature and search index randomizations.

IV. SELECTIVE ENCRYPTION ALGORITHIM

[16]Every encryption process requires an encryption algorithm and a key to encrypt particular data. In Selective encryption, key is generated before the process of encryption and decryption instead of storing it. In secure communication, key generation phase has many challenges and this problem can be solved if the sender and the receiver share the key in any other form or if they generate the keys readily during encryption and decryption separately.

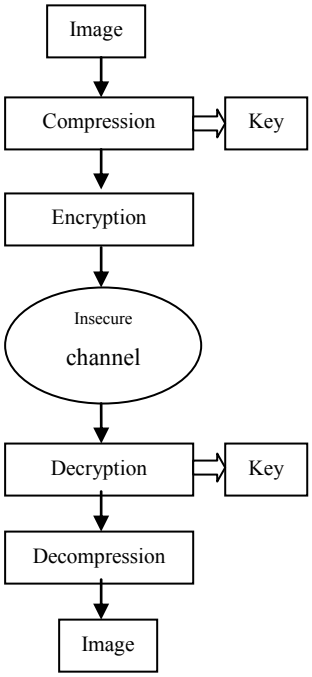

Fig 2 : Encryption of Images

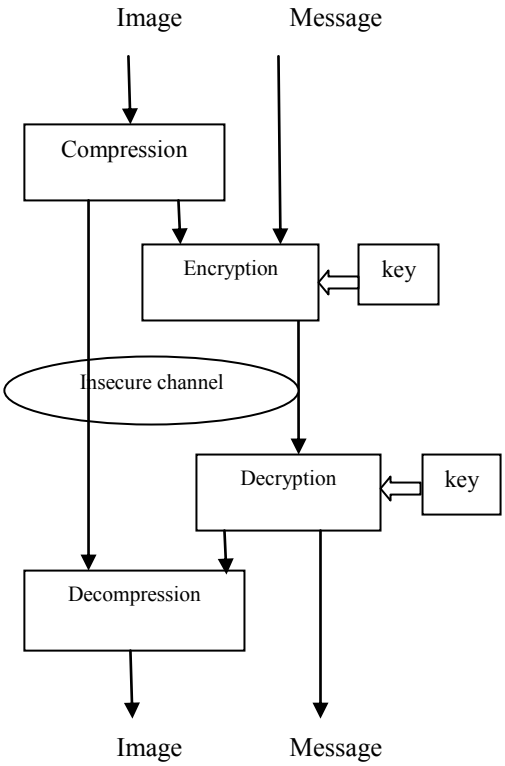

Fig 3: Selective Encryption Technique

From Fig. 2, it is clear that the receiver should decrypt the information before it can decompress the image. This approach has the main drawback that it is impossible to access the smallest part of information without knowledge of the key. For example, it would impossible to search through a general database of fully encrypted images. A way to address this issue is to use a technique called selective encryption; it is depicted in Fig. 3. The image is first compressed if needed .Afterwards the algorithm only encrypts part of the bit stream with a well-proven ciphering technique; incidentally a message can be added during this

process. To guarantee a full compatibility with any decoder, the bit stream should only be altered at places where it does not compromise the compliance to the original format. This principle is sometimes referred to as format compliance.

V .BLOCK-BASED TRANSFORMATION ALGORITHM

In, block-based transformation algorithm the transformation technique works as follows: original image is divided into a random number of blocks that are then shuffled within the image. The generated image is then fed to the Blowfish encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks.

VI. BlOWFISH ALGORITHM

[18] Blowish f. algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security. As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. This operation is different from the permutation function performed in DES.

VII. EXPERIMENAL RESULTS

Image encryption and decryption algorithm is developed in matlab. In the first step we take any image which we want to encrypt and apply any key consist of number. When we want to decrypt this image we need to enter same key. If we provide wrong key then image will not decrypt.

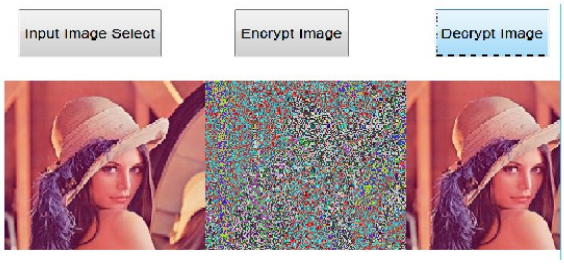

Fig 4: Selective Encryption Algorithm

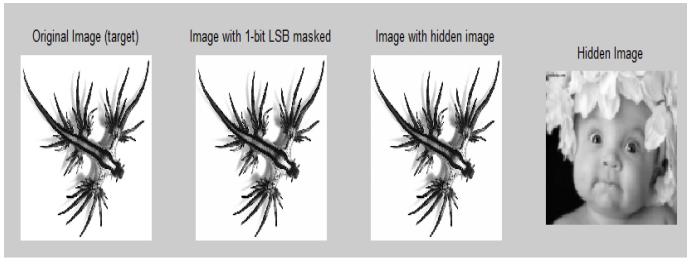

Fig 5 : Block-Based Transformation Algorithm

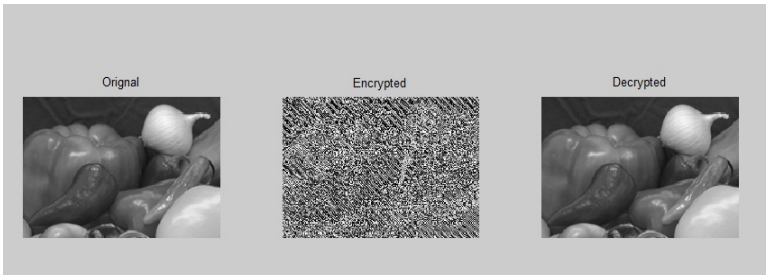

Fig 6 : Blowfish Algorithm

CONCLUSION

In this paper a simple and strong method has been proposed for image security using a combination of block based image transformation encryption techniques. Selective encryption algorithm. and Blowfish algorithm.

REFERENCES

[1]P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications', IEEE Transactions on Consumer Electronics, voI.46,no.3,pp.395-403, Aug.2000.
[2] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuit and Systems, ISCAS 2002. IEEE International.
[3]Siddharth Malik, Anjali Sardana and Jaya, "A Keyless Approachto Image Encryption", IEEE 2012 International Conference on Communication Systems and Network Technologies (2012), 879-88, Symposium on Publication Date: 2002, Vol. 2,2002, page(s):708,711.
[4] Li. Shujun, Li. Chengqing, C. Guanrong, Fellow., IEEE., Dan Zhang., and Nikolaos,G., Bourbakis Fellow., IEEE. "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004, http://eprint.iacr. Org/2004/374.pdf
[5]Q.Hua Lin, Fu-Liang Yin, and Y.R. Zheng" Secure image communication using blind source separation" 2004 IEEE.
[6]Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.
[7]K.C. Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" 1-424-0220-4/06 ©2006 IEEE.
[8] M. Sabery.K, M.Yaghoobi, "A New Approach for Image encryption using Chaotic logistic map", 978-0-7695-3489-3/08 © 2008 IEEE.
[9]Tingyuan Nie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009
[10]W. Lu, A. L. Varna, A. Swaminathan, and M.Wu, ``Secure image retrieval through feature protection," in Proc. IEEE Conf. Acoust., Speech Signal Process., Apr. 2009, pp. 1533_1536.
[11] Jing Qiu and Ping Wang, " Image encryption and authentication scheme", IEEE, Computational Intelligence and Security (CIS), 2011 Seventh International Conference, 3-4 Dec.
[12] Xinpeng Zhang "Separable Reversible Data Hiding in Encrypted Image" IEEE transactions on information

forensics and security, vol. 7, no. 2, april 2012
[13] Jianji Wang, Student Member, IEEE, and Nanning Zheng, Fellow, IEEE"A Novel Fractal Image Compression Schemewith Block Classification and Sorting Basedon Pearson's Correlation Coefficient" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 9, SEPTEMBER 2013
[14]Tawfiq S. Barhoom, Zakaria M. Abusilmiyeh, "A Novel Cryptography Method Based on Image for Key Generation", In "2013 Palestinian International Conference on Information and Communication Technology", 2013 IEEE, P.N. 71-76.
[15] wenjun lu1, avinash l. varna2, (member, ieee), and min wu3, (fellow, ieee) "A Comparative Study Between HomomorphicEncryption and Distance-Preserving Randomization.", VOLUME 2, 2014 IEEE.
[16] Abhishek Thakur1, Rajesh Kumar2, Amandeep Bath3, Jitender Sharma4 "Design of Selective Encryption Scheme Using Matlab", IJEEE, Vol. 1, Issue 1 (Jan-Feb 2014)
[17]Mohammad Ali Bani Younes and Aman JantanImage "Encryption Using Block-Based Transformation Algorithm" IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03
[18] Pia Singh Prof. Karamjeet Singh "image encryption and decryption using blowfish algorithm in matlab" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 150 ISSN 2229-5518

