ISSN:0975-9646

Review on Block Based Transformation Image Encryption Techniques

Himani Patwa and Akhilesh Deep Arya
Techno India NJR Institute of Technology, Udaipur (Raj.) - 313001

Abstract-Internet has become part and parcel in today's scenario. Internet is a public network and is not so secure for the transmission of confidential content. With the fast progress in digital data exchange and increased usage of multi media images, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. Block transformation is a beneficial approach to secure the image data by shuffling the pixels of the image into a jumbled format. The relationship between the pixels of image is very strong. Block transformation eliminates the image outlines and dissipate the high correlation among image pixels.

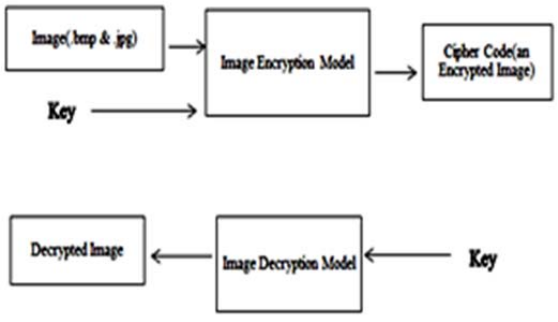
INTRODUCTION

Due to growth in network technology the exchange of digitals images has increased very significantly. Hence the probability of replication of digital images and their redistribution by hackers is more susceptible. Therefore the images should be transferred protectively.

Image Encryption provides us a technique which secures the images by converting the original image to a ciphered image which is very difficult to understand. Encryption transforms the information by using an encryption algorithm so that it becomes difficult to understand for everybody except those who possess the shared or the secret key. By undertaking such procedure, the encrypted information is obtained which is referred to as cipher text. The reverse process is the decryption process.

Architecture Of Image Encryption Model

For encryption and decryption a symmetric key model has been used. The architecture of image encryption and decryption model is described in Figure –1



Architecture of Image Encryption and Decryption Model

Categories Of Image Encryption Techniques

Encryption techniques are usually characterized into following three:

Position permutation techniques: This technique changes the arrangement of pixels which completely changes the image.

Value transformation techniques: Chaotic system is used in this technique that generates a binary sequence, according to that the weights and biases of the network are set.

Combination: This technique combines position permutation and value transformation techniques. Position permutation will rearrange the pixels and then value transformation technique will replace the pixel values using a key generator.

Performance Parameter Of Image Encryption

There are some few parameters on which encryption technique is evaluated.

Visual Deprivation (VF): This parameter measures perceptual alteration of image data with reference to the original image. In case of highly sensitive data for complete masking of visual content the visual deprivation parameter should be kept high.

Compression Responsiveness (CR): Few encryption schemes influence data compressibility or infuse further data which is required for decryption. If an encryption technique has very slight or no influence on data compression productivity than it is considered as compression responsive.

Encryption Ratio (ER): Amount of data which is to be encrypted is measured by this parameter. To cut computational complexity encryption ratio has to be lessened.

Speed (S): The encryption and decryption algorithms must be fast enough to meet the real time requirements in case of real time systems.

Cryptographic Security (CS): This parameter measures the security level of the encryption pattern against brute force and another plaintext –cipher text attacks. In case of confidential multimedia applications, is becomes very important that the cryptographic security parameter is satisfied.

LITERATURE REVIEW

The idea behind encrypting an image is to transfer the image over the network without being attacked by any unauthorized user. There is a big difference between text and image encryption. Image data has some different properties like high redundancy, bulk capacity and high correlation between the pixels which enforces some added requirements on any cryptographic technique.

Mahmood Al-khassaweneh and Selin Aviyente [1] in their paper have given an image encryption technique which is

based on Least Square Approximation (LSA). This paper offers the conversion of the original image into the form of vectors which are generated one by one randomly. Alternatively the decryption is performed using LSA on encrypted image and also on the randomly generated vectors. This algorithm enhances the security and also provides a good range of efficiency.

Abugharsa et al. [4] proposed another approach for image encryption which is based on shifting the columns and rows of an image. This methodology uses a shifting table which is generated by some hash function. The image is divided into the blocks of 3 * 3 pixel values then these blocks are transformed before encryption. The correlation value among the original image and ciphered image is -0.0078 which shows strong correlation among original and ciphered image. This indicates that the neighbourhood pixels in the original image have nearest value than the neighbourhood pixels of the encrypted image, this show a good sign that the probability is low. Though the entropy value is observed high it can be said that the security provided by this technique is low.

Another image encryption technique is proposed by De Wang, Yuan-Biao Zhang [2] which is based on S-box Substitution and Chaos theory. This technique involves of two steps. The first step practises S-box for substitution of each byte and it includes multiple rounds of S-box substitution. In the next step a random sequence chaotic algorithm is applied. This improved algorithm enhances efficiency and can easily be implemented.

Panduranga et al. [3] proposed two methods that can be used for image encryption. The first method divides the image into random number of blocks. These blocks are encrypted using image mapping which is used as input to these blocks. Encryption of selected blocks can also be done then each image can use distinct map image. In another proposed method, the location of items in a given image is identified inevitably using morphological techniques, which trace the locations of the items of the given image. Then encryption is applied on the information taken out from the detected item of the image. These techniques are appropriate for some special applications like medical images and satellite image.

PROPOSED WORK

The encryption algorithm is divided into two phases i.e. block dividing of fixed size then rearrange the blocks and at last applying some transformation algorithm. The working of the proposed encryption algorithm is explained in the following steps:

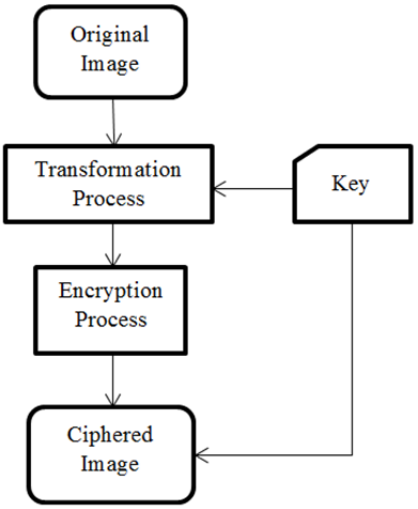
Step 1: Input Image

Step 2: Block Based Transformation:

i) Divide the input image into equal size blocks,

ii) Shuffle the blocks using affine transformation so the correlation between the neighbour pixel decreases,

iii) Output encrypted image.



CONCLUSION

This paper reviewed the existing image encryption techniques and analysed them to endorse the performance parameters like cryptographic security, compression ratio etc. Each technique is exclusive, which might be appropriate for different applications. New encryption techniques are evolving is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security**.**

REFERENCES

[1] Mahmood Al-khassaweneh, Selin Aviyente,"Image Encryption Scheme Based on Using Least Square Approximation Techniques" IEEE Transactions, pp.108-111, 2008.

[2] DeWang, Yuan-Biao Zhang, "image encryption algorithm based on s-boxes substitution and chaos random sequence", International Conference on Computer Modeling and Simulation, 2009 IEEE.

[3] H. T. Panduranga, and S. K. Naveen Kumar, "Selective image encryption for Medical and Satellite Images", International Journal of Engineering and Technology (IJET), vol. 5, no. 1, 2013, pp. 115–121.

[4] Ahmed Bashir Abugharsa, Abd Samad Bin HasanBasari and Hamida Almangush "A New Image Encryption Approach using Block-Based on Shifted Algorithm", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.12, December 2011.

[5] Mohammad Ali Bani Younes and Aman Jantan Image Encryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35, 2008