ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

DSC and LPDC Based Reversible Data Hiding

S.Kalpana[1], S.Vinothini[2]

Assistant Professor, Dept. of ECE, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu, India[1]

PG Student [CS], Dept. of ECE, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu, India[2]

ABSTRACT: Security is the main concern in today's world and securing data from unauthorized access is very important. Different techniques should be used to protect confidential image data from unauthorized access as each type of data has its own features. In the natural images the values of the neighbouring pixels are strongly correlated. Correlation means that the value of any given pixel can be reasonably predicted from the values of its neighbours. The proposed technique "secure image data by double encryption" provides image data security using cryptographic technique. The proposed method breaks the correlation among neighbouring pixel by dividing original image into blocks of size of n pixels*n pixels (n is provided by user) and then encrypt each pixel by their position (x, y) and then encrypt each block by AES Encryption algorithm by using public key of the receiver. The result shows that the correlation between image pixels is decreased and higher entropy is achieved by using this technique.

KEYWORDS*:* Cryptographic technique, Security image, most significant error.

I.INTRODUCTION

Government, military, financial institution, hospitals and private businesses amass great deal of confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defence), product, and financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer, if these confidential images about enemy positions ,patient ,and geographical areas fall into the wrong hands, than such a breach of security could lead to lots of war , wrong treatment etc. Protecting confidential images is an ethical and legal requirement.

We store information in computer system in the form of files. File is considered as a basic entity for keeping the information. Therefore the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is word wide accepted fact that securing file data is very important, in today's computing environment [3]. There are n numbers of approaches available to persuade image file data security, but due to large data size and real time Constrains, algorithms that are good for textual data may not be suitable for multimedia data.

There are various approaches available to ensure file data security, such as encryption tool like "aescrypt" for text and other chaos based encryption application for image, but each one has its own disadvantage, rendering them being less frequently used.

In this paper we are introducing a new algorithm of image data security, Secure Image Data by the encryption of image data double, first encrypt is of pixel by their position (x, y) and second encryption is of each block. There is a world of difference between digital images data and texts data in many aspects and thus required different encryption technique. In the natural images, the values of the two neighbour pixels are strongly related to each other. I.e. if we have the value of any one of the pixel than we can easily predict the value of other one pixel (called correlation among pixels). With the aim to reduce this high correlation between pixels and to increase the entropy value, we are proposing a Secure Image Data by using a combination of double encryption process based on the combination of the encryption by pixel position (x, y) and another encryption for the blocks. We are using public key cryptography which is a worldwide known encryption algorithm. The transformation process that we are using is used to divide the original image into a number of blocks that are then encrypted by their pixel position with one other within the image. The resultant image is then become the input to the public key encryption algorithm. By tacking the correlation and entropy as a parameter of security, the encryption process by their pixel position will be expected to result in a lower correlation and a higher entropy value when compared to using the An Image encryption approach using a combination of permutation Technique followed by encryption and thus improving the security level of the encrypted images. We are using the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

concept of public key encryption, for the encryption and decryption of image. In this public key's of sender and receiver is known to both but private key's are kept secret

II.EXISTING SYSTEM AND ENCRYPTION

We are using a separable reversible data hiding method for encrypted images using Slepian-Wolf source encoding. The idea is inspired by the Distributed source coding (DSC), in which we encode the selected bits taken from the stream-ciphered image using Low density parity check LDPC codes into syndrome bits to make spare room to accommodate the secret data. With two different keys, the proposed method is separable. The hidden data can be completely extracted using the embedding key, and the original image can be approximately reconstructed with high quality using the encryption key. With both keys available, the hidden data can be completely extracted, and the original image perfectly recovered with the aid of some estimated side information.

RESERVING ROOM BEFORE ENCRYPTION (RRBE)

The new idea in reversible data hiding is implemented as shown in fig1, Reserving Room before Encryption (RRBE). Standard RDH algorithms are used for reserving room in RRBE to achieve better performance. All the previous method uses the technique of Vacating Room after Encryption (VRAE). It empty out the room from the encrypted image. In Vacating Room after Encryption content owner first encrypts the original image using an encryption key. After that content owner reserves space on the original image and send it to the data hider by embedding data into the encrypted image. This method cannot provide good image quality and also real reversibility is not achieved in this case. But in RRBE first content owner reserves space on the original image. Various RDH methods are used for reserving space in the original image. Then the image is encrypted by using an encryption key. This encrypted image is sent to the data hider for embedding additional data. So the encrypted images with the embedded information are sending to the receiver side. At the receiver side, data's are recovered by using data hiding key and encryption key. Reserving Room before Encryption consists of reserving room in image, encryption of image, data embedding in encrypted image, extraction of data and image recovery. To reserve room in an image various RDH techniques are used.LSB replacement, difference expansion, histogram shift are the various RDH techniques.

VACATING ROOM AFTER ENCRYPTION (VRAE)

A content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by loss lessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key. In all methods the encrypted 8-bit gray-scale images are generated by encrypting every bit-plane with a stream cipher. The method in segments the encrypted image into a number of non overlapping blocks sized by; each block is used to carry one additional bit. To do this, pixels in each block are pseudo-randomly divided into two sets and according to a data hiding key. If the additional bit to be embedded is 0, flip the 3 LSBs of each encrypted pixel in , otherwise flip the 3 encrypted LSBs of pixels in . For data extraction and image recovery, the receiver flips all the three LSBs of pixels in to form a new decrypted block, and flips all the three LSBs of pixels in to form another new block; one of them will be decrypted to the original block. Due to spatial correlation in natural images, original block is presumed to be much smoother than interfered block and embedded bit can be extracted correspondingly. However, there is a risk of defeat of bit extraction and image recovery when divided block is relatively small (e.g.,) or has much fine-detailed textures. Reduced the error rate of Zhang's method by fully exploiting the pixels in calculating the smoothness of each block and using side match. The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks and recovered blocks can further be used to evaluate the smoothness of unrecovered blocks, which is referred to as side match. Zhang's method in pseudo-randomly permuted and divided encrypted image into a number of groups with size of. The LSB-planes of each group are compressed with a parity-check matrix and the vacated room is used to embed data.

III.DATA HIDING

Data hiding are a group of techniques used to put a secure data in a host media (like images) with small deterioration in host and the means to extract the secure data afterwards. For example, steganography can be named. Steganography is one such pro-security innovation in which secret data is embedded in a cover. But, this paper will get into reversible

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

data hiding. Reversible data-hidings insert information bits by modifying the host signal, but enable the exact (lossless) restoration of the original host signal after extracting the embedded information. Sometimes, expressions like distortion-free, invertible, lossless or erasable watermarking are used as synonyms for reversible watermarking. In most applications, the small distortion due to the data embedding is usually tolerable. However, the possibility of recovering the exact original image is a desirable property in many fields, like legal, medical and military imaging. Let us consider that sensitive documents (like bank checks) are scanned, protected with an authentication scheme based on a reversible data hiding, and sent through the Internet. In most cases, the watermarked documents will be sufficient to distinguish unambiguously the contents of the documents. However, if any uncertainty arises, the possibility of recovering the original unmarked document is very interesting. Lossless data embedding techniques may be classified into one of the following two categories: Type I algorithms employ additive spread spectrum techniques, where a spread spectrum signal corresponding to the information payload is superimposed on the host in the embedding phase. At the decoder, detection of the embedded information is followed by a restoration step where watermark signal is removed, i.e. subtracted, to restore the original host signal. Potential problems associated with the limited range of values in the digital representation of the host signal, e.g. overflows and underflows during addition and subtraction, are prevented by adopting modulo arithmetic. Payload extraction in Type-I algorithms is robust. On the other hand, modulo arithmetic may cause disturbing salt-and-pepper artefacts. In Type II algorithms information bits are embedded by modifying, e.g. overwriting, selected features (portions) of the host signal -for instance least significant bits or high frequency wavelet coefficients-. Since the embedding function is inherently irreversible, recovery of the original host is achieved by compressing the original features and transmitting the compressed bit-stream as a part of the embedded payload. At the decoder, the embedded payload- including the compressed bit-stream- is extracted, and original host signal is restored by replacing the modified features with the decompressed original features. In general, Type II algorithms do not cause salt-and-pepper artifacts and can facilitate higher embedding capacities, albeit at the loss of the robustness of the first group.

IV.IMAGE ENCRYPTION TECHNIQUES

SCAN BASED IMAGE ENCRYPTION

The SCAN is a formal language based on two dimensional spatial accessing methodologies which can represent and generate a large number of wide variety of scanning paths or space filling curves easily. There are a family of formal languages such as Simple SCAN, Extended SCAN, and Generalized SCAN, each of which can represent and generate a specific set of scanning paths. It is first employed for image encryption. The plain image is initially serialized to one dimensional data stream which is then described by the SCAN language. Several scanning orders are expressed into the corresponding SCAN letters. Combinations of SCAN letters from different kinds of secret images. The SCAN string is served as an encryption key bound to a given 2D image array. The encryption procedure is to rearrange image into a final sequential representation. Each assembled secret image in process of SCAN string is combined by the insertion of additive noises at particular image points. Since no one except the intended user can obtain the correct SCAN combinations, the original image is therefore considered confidential.

SELECTIVE BIT PLANE ENCRYPTION

Intuitively, SE seems to be a good idea in any case since it is always desirable to reduce the computational demand involved in image processing applications. However, the security of such schemes is always lower as compared to full encryption. The only reasons to accept this drawback are significant savings in terms of processing time or power. Therefore, the environment in which SE should be applied needs to be investigated thoroughly in order to decide whether its use is sensible or not. Due to requirements of certain applications a loss of image quality may not be acceptable during transmission or storage (e.g., in medical applications because of reasons related to legal aspects and diagnosis accuracy). Lossless compression schemes need to be employed for such applications. We assume a target environment, where due to the low processing power of the involved hardware not even lossless compression and decompression of visual data is reasonable or possible (e.g. mobile clients). Additionally, due to the increasing bandwidth available at mobile communication channels, compression seems not to be mandatory in any case, which is especially true for lossless applications. The reason is that the data reduction of lossless compression schemes is much lower as compared to lossy ones making the respective application less profitable. Note also that the time demand for compression is significantly higher as the time demand for encryption for almost all high quality codecs and symmetrical ciphers (which is mostly due to the efficient cache use of block-based encryption).

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

EMBEDDING IMAGE COMPRESSION INTO ENCRYPTION

The above mentioned schemes are devoted to the uncompressed image data. For compressed images, some special measures are required before strictly combining encryption and compression directly. A framework is proposed for fast encryption by entropy encoders such as Huffman coder. In entropy coding, the statistical model is used to decode the compressed bit stream. It is therefore suggested that multiple statistical models are used alternately in certain secret order to encode the input symbol stream. Through security analyses, this scheme is proved to be applied effectively on both multiple Huffman coding tables of Huffman coder and multiple state indices of QM coder. However, it should be noted that the original image can be correctly reconstructed only if its input is identical to the output of the encoder. There is also a concern about codec dependence of such kind of scheme. Nevertheless, the potential for integrating encryption with multimedia compression at a low computation is promised.

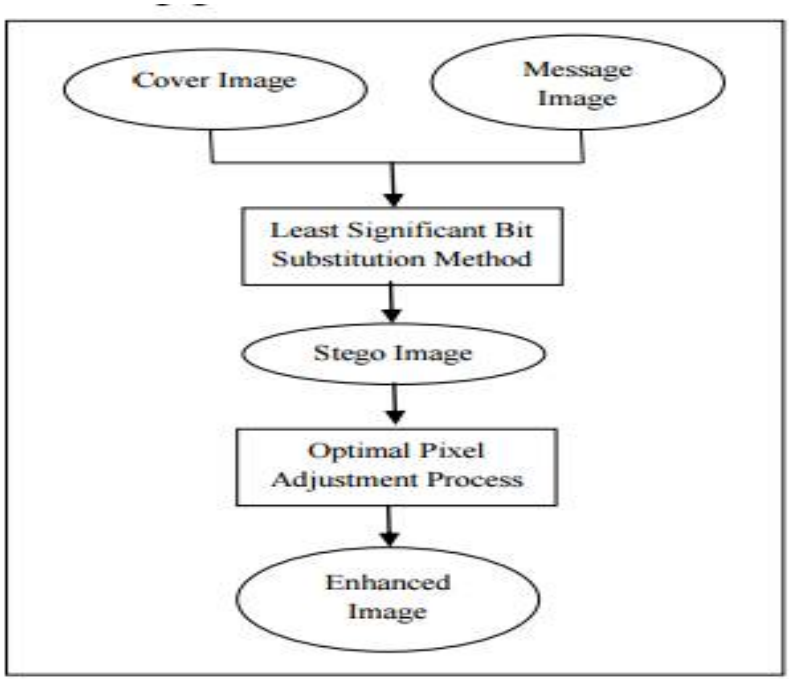

Fig 1. Image Hiding Mechanism

IMAGE ENCRYPTION USING CHAOTIC MAP

Chaos signals are considered good for practical use because they have important characteristics such as they are highly sensitive to initial conditions and system parameters, they have pseudo-random property and non periodicity as the chaotic signals usually noise-like, etc. Consequently, the combination of chaotic theory and cryptography forms an important field of information security. Chaos theory has been established by many different research areas, such as physics, mathematics, engineering, and biology. Since last decade, many researchers have noticed that there exists the close relationship between chaos and cryptography. Point out an image encryption scheme which utilizing two chaotic logistic maps and an external key of 80-bit. The initial conditions for both logistic maps were obtained from the external secret key. The first logistic map was used to generate numbers in the range between 1 and 24. The authors showed that by modifying the initial condition of the second logistic map in such a way that its dynamics became more random. Suggest an encryption method called BRIE based on chaotic logistic map. The basic principle of BRIE is bit recirculation of pixels, which is controlled by a chaotic pseudo random binary sequence. The secret key of BRIE consists of two integers and an initial condition of the logistic map. Presented a novel pixel-based scrambling scheme to protect and secure way, the distribution of digital medical images. To provide an efficient encryption of a large volume of digital medical images, the proposed system uses simple pixel level XOR operation for image scrambling in an innovative way such that structural parameters of the encryption scheme have become a part of the cryptographic key

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

V. RESULT AND DISCUSSION

In the fig 2,the input image has been implemented as original image and it modified to be an encrypted image and also in an input image has recover in an modified in output image without change.

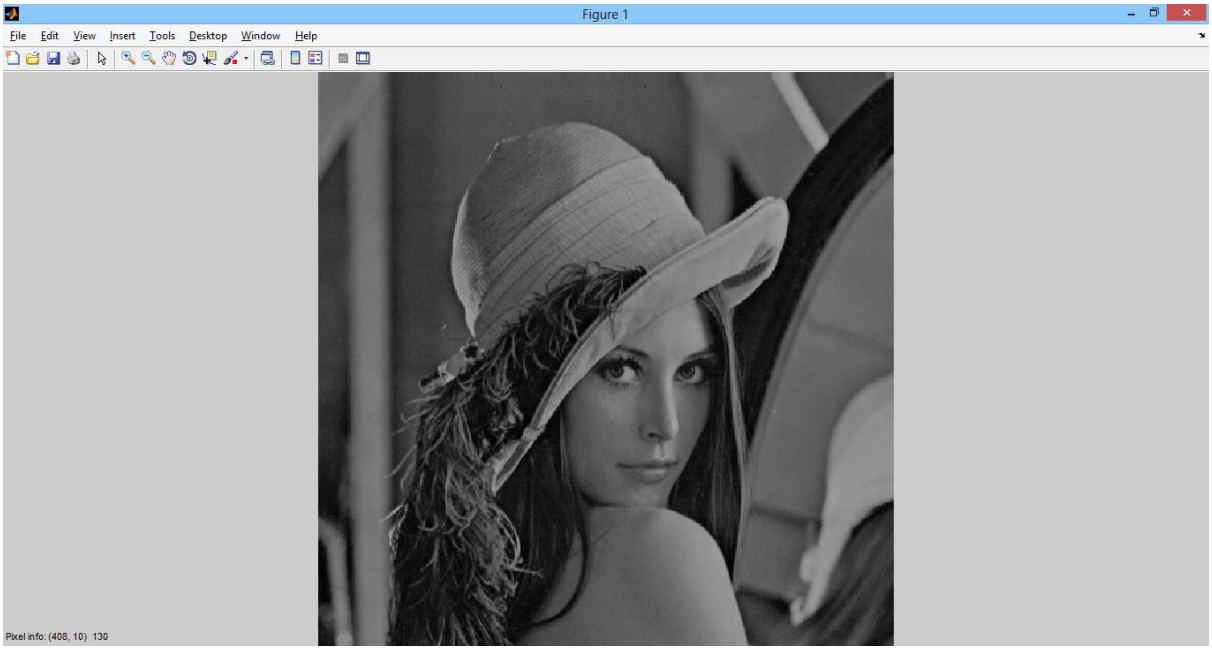

Fig. 2 Input Image

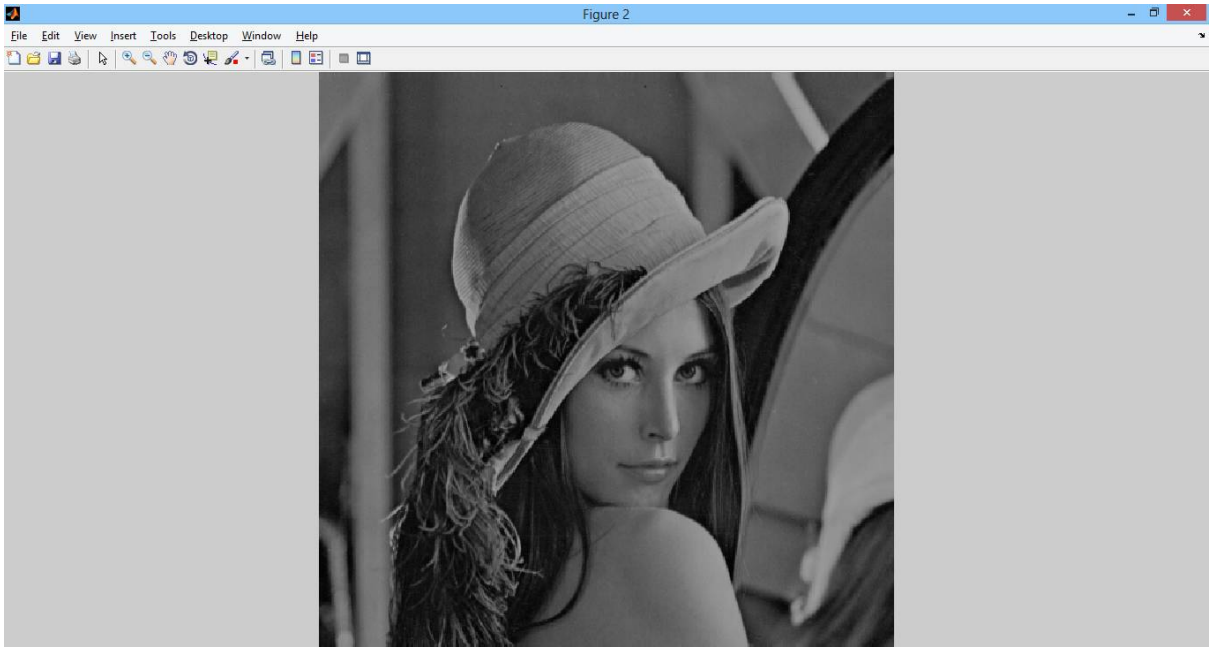

Fig. 3 Encrypted image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

In the fig 3, the input image will be encrypted two times by use of RSA and OPAP algorithm; by the way of two times encryption the image has been secured high.

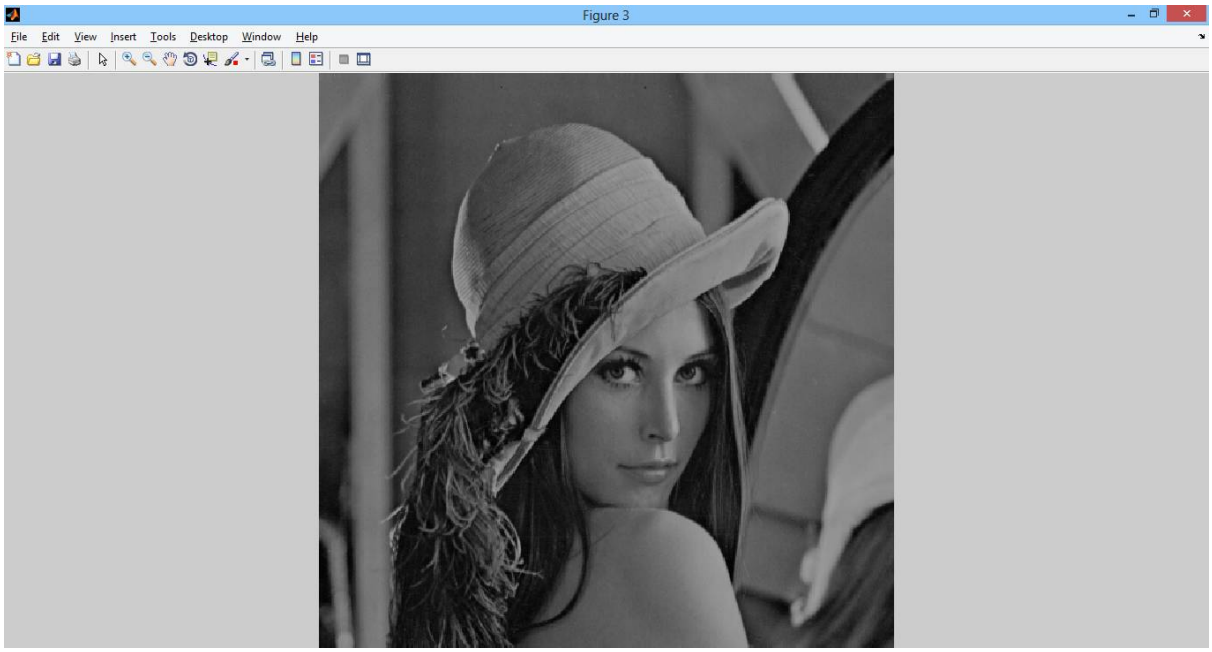

Fig .4 Output image

In Fig 3,this output image, the image will get high PSNR rate and the quality will be high, When hide the data or message in an image format, this image format will using two time encryption method no one can hack the data. The output image has been recovered as composed image.

VI.CONCLUSION

This paper presents a technique "Secure Image Data by Double Encryption" for image encryption and decryption. This will provide a valuable tool for secure image transfer. It is very unsecure to transfer an image without breaking the correlation among adjacent pixels, due to strong correlation among neighbouring pixels; the proposed encryption technique will decrease the correlation and increase the entropy of the image. To make a secure image system, the proposed technique divides an image into blocks of n*n size and then perform double encryption process, this will decrease the correlation among neighbouring pixels and increase the entropy and transform the block into encrypted form.

REFERENCES

[1] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block – Based Transformation Algorithm" IAENG, 35:1, IJCS_35_1_03, February 2008.
[2] Mohammad Ali Bani Younes and Aman Jantan, "An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS, vol 3 no 4, April 2008
[3] Rajesh Kumar Pal and Indranil Sengupta, "Enhancing File Data Security In Linux Operating System by Integrating Secure File System" June 2009.
[4] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom
[5] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), 1229-1245
[6] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encr-yption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China
[7] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm" Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China,E-mail: jcyen@mail.lctc.edu.tw.