Volume 2, Issue 6 June 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

IRJIF IMPACT FACTOR: 3.01

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

REVIEW ON IMAGE DATA ENCRYTION TECHNIQUES: A BRIEF SURVEY

RIPANJOT ANETA[1] MRS. APOORVA[2]

[1]M.tech Student (CSE), CEC Landran, Mohali, India
[2]Assist. Prof. (CSE), CEC Landran, Mohali, India

ABSTRACT-

Digital Encryption has become the important area of reaseach with the rapid development in this area in the recent years.Security of data and the copyright protection are the important issue in the field of media development and the adminstartion work. For preventing the illegal manipulation and safely transmition of images of data over the network, the new technology image encryption has been devloped. Image encryption deals with the embedding the copyright information into the stream of image bits.Techniques for encrypting the image sequence are same as that of teh techniques used for the image encryption.But however image encryption technique also handles some issues that are not considered while encrypting the image. In this paper, survey of various available techniques for image encrytion has been done to provide the critical review of the avialable techniques.

Keywords- ***Image Encrypting, Singular Value Decomposition (SVD), Robustness, Imperceptibility, Human Visual System.***

I. INTRODUCTION

With the advancement of technology the transfer of images, images, music, pictures, and textual data has become easier over the network [1]. Due the advancement of the transfer of data over the internet has become effortlessly open and simple; anybody can access the data of other if the security of data is not being implemented. Copyright protection provides the copyright to the authorised user of the data. By doing so the authorised data is prevented from unauthorized access [2]. Encryption and decryption are the main concern in today's world. As encryption and decryption techniques are not fast enough to deal with the large amount of data to be encrypted and decrypted. Quality and size of image is needed to be preserved while encrypting and decrypting the data. Partial encryption deals with the method of encrypting the lowest portion of the data to reduce the computation of the system and hence reducing the encrypting time for the algorithm [3].

Encryption deals with converting the data from plain data to the cipher data by encryption key technique i.e. assigning the key to the data .when the data

reaches its destination it is decrypted by using the key. Decryption key convert the cipher data to the plain data as before. Keys can be classified into two categories symmetric and asymmetric key algorithm. In symmetric key encryption private key is used for encrypting the data whereas in asymmetric key encryption two different keys are used for encrypting and decrypting the data. Public key is used for the encryption and private key is used for decrypting the data [4].Encryption should be crystalline in nature so that the quality of the data remains the same and is being undetectable for the unauthorised user.

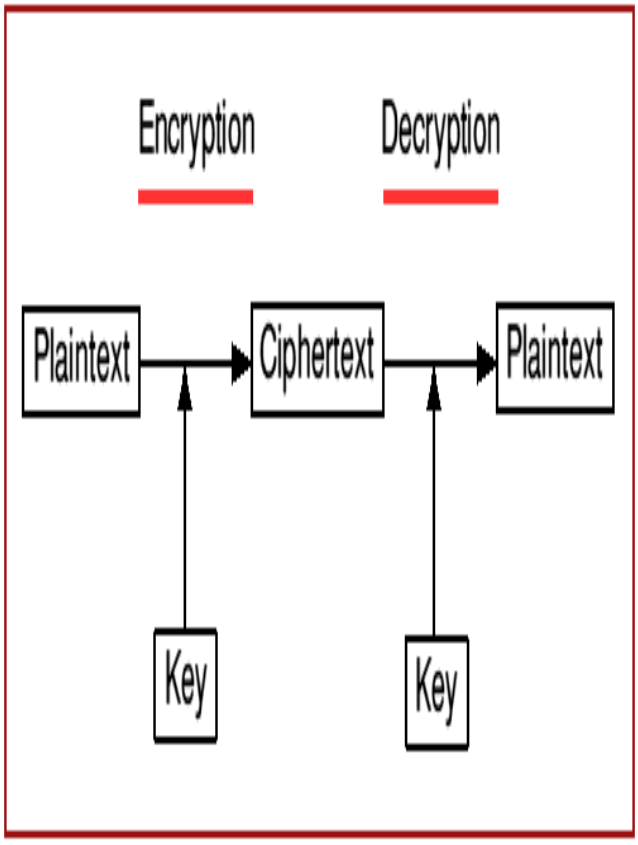

Figure1. Encrypting Process

II. IMAGE ENCRYPTING

Since the large amount of data is being transferred over the internet in many forms such as internet images, wireless images, conferencing over the image leads to many problems such as unauthorized access by different authors over the internet. So techniques are developed to provide the security to the transfer of images over the internet. Copyright provides the ability to provide the authorised access to the user of the data. Use of copyright is general in the audio image industry. Research has been done to provide the security over the internet. Researchers have made possible to provide the methods so as to prevent the illegal copying and manipulation of the data [6]. Figure show that the Encryption technique can be classified into four types according to their use. They are domain, document, perception and application. On the basis of domain the Encryption technique can be classified into the two domains i.e. spatial domain and frequency domain. On the basis of documents Encryption can be categorized into various types of documents such as audio, image, text and images. On the basis perception Encryption can be categorized into Invisible and visible type of encryption. On the basis of applications Encryption can be divided into two categories i.e. source based applications and destination based application.

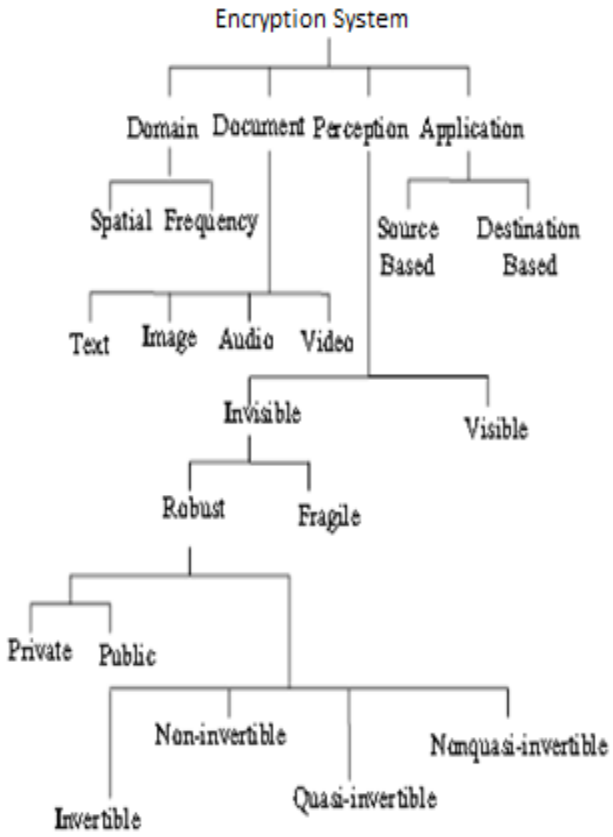

Figure 2. Encrypting Types

III. IMAGE ENCRYPTING TERMINOLOGIES:

Images are embedded with information by the process of image encryption so as to provide the security to the images over the network. Various terminologies used in image encryption are [8]

Digital Image: image sequence refers to the collection of still pictures that are moved at such a fast speed that human eye perceives that they are actually moving. Basically the image sequence is collection of frames.

Payload: payload refers to the amount of the data that can be encrypted in particular frame. Basically the payload of the image sequence is the encryption granularity. Encryption granularity deals with specifying the amount of information required to insert in the one unit of encrypted data.

Perceptibility: Perceptibility deals with the recognition of the original image in the image encryption. Since it becomes vague if this property of the data is not fulfilled.

Robustness: Robustness property of the image encryption deals with providing the security to the image data from all the users. Data should remain secure however it is subjected to the authorized or unauthorized users. According to the various applications the encryption can be categorized into various categories such as robust, fragile and semi fragile.

Security: Security refers to the phenomenon of providing the surety that information would not be Lost, alerted or modified, by using the image encryption technique. Security largely depends on the fact of type of key that has been used for encrypting the data.

IV. SURVEY OF TECHNIQUES

In the previous years, various encryption algorithms have been proposed to provide the security to the data

from the unauthorized access. Features of data are encrypted by using the feature encryption methodologies to secure the data. It can be classified into two categories i.e. spatial space encryption and convert area encryption.

Spatial space encryption deals with encrypting the spatial area by changing the pixel values of each edge to secure the data. Spatial encryption follows difficult procedures to encrypt the data.

Various methods have been used to twist the recurrence area of the encryption. Encryption is performed to provide the security to the data from the intruders, this can be done by the various methods such as edge averaging, swapping of casing, digital analog transformation, and transformation operations for the recurrence area. Various transforms associated with the encryption are discrete fourier transform (DFT), the discrete cosine transform (DCT), and the discrete wavelet transform (DWT).

Least Significant Bit Modification

Least significant bit modification technique is simple and straightforward technique that deals with the use of least significant bits to be embedded by the system for the encryption purpose. This technique provides the high capacity to embed the data. Cropping of the data is forbidden by using this technique however least significant bit technique is fragile to the addition of noise into the algorithm, compression and resetting the values of the least significant bits [10]. However there are many drawbacks of this technique, this technique is unable to handle the cropping of the data, lossy compression of the data and addition of noise deteriorates the performance of this algorithm. By using LSB technique it makes the little impact on the cover object. The encryption performed by this technique can be easily modified by the intermediate party. An approach to enhance the robustness is to applying a pseudo random generator to determine the LSB bits to modify. By the use of this technique along with LSB the intermediate party is prevented to access the encrypted data hence provide the security to the data.LSB method of encryption is very simple and powerful method of encrypting the data so it is widely used in the field of stenography. However this techniques does not contain the robustness feature it has been widely used for encrypting the data to make it secure.

Correlation-Based Techniques

Correlation technique of encryption deals with encrypting the data by using the correlation properties to embedding along with the pseudo random noise pattern. A pseudo-random noise (PN) pattern W(x, y) is added to the cover image I(x,y), according to the equation shown below in Equation 1.

$$Iw(x, y) = I(x, y) + k \times W(x, y) \qquad (1)$$

In Equation 1, k denotes a gain factor, and IW the resulting encrypted image. Robustness is increased by the increase in the value of k however the quality of the encrypted image is affected. For retrieving the original image after the encryption same pseudo-random noise generator algorithm is used along with the same key .correlation between the encrypted image and the noise pattern is examined or providing the better level of security. This algorithm works by checking the value of threshold and each time single bit is set to indicate the encryption,.

Discrete Cosine Transform

Discrete cosine transform is used to encrypt the data to provide the security. In DCT image is split up into various recursive groups and then performing the encryption into the centre recursive. Centre groups are picked so as to provide and reduce the strategic distance from the other part of the image. Discrete cosine transform is used to represent the image in the form of cosine function. Discrete cosine transformation can be classified into two categories global DCT encrypting and block based DCT encrypting. DCT encryption is based on the procedure of the discrete transform. Low pass sifting, brilliance; contrast change and obscuring are used in the discrete cosine transform to provide efficient results.

Discrete Wavelet Transform

Discrete wavelet transform is used structure the sines and cosines to solve the problems of the Fourier transformations. Recurrence is changed in each step in the DWT. Recurrence is moved between the low recurrence and high recurrence. Various bands in discrete wavelet transform are LL bands that deals with the low recurrence, LH band that deals with the flat high recurrence band, HL band that deals with the vertical high recurrence band, HH deals with the inclining high recurrence band.

In discrete wavelet transform the most noticeable data is considered having the high amplitude and low amplitude is shown by the less noticeable data. Information can be easily gathered by checking the amplitude values. Wavelet transform is efficient as it maintains the measure of time frequency measurement and the recurrence data.

DWT is the most accepted part of the human visual system as the values are easily read by the human.

Human visual system is less delicate to the encryption of the data. Discrete wavelet transform has been developed to handle the various types of assaults when the insertion is made in the LL part of the DWT.

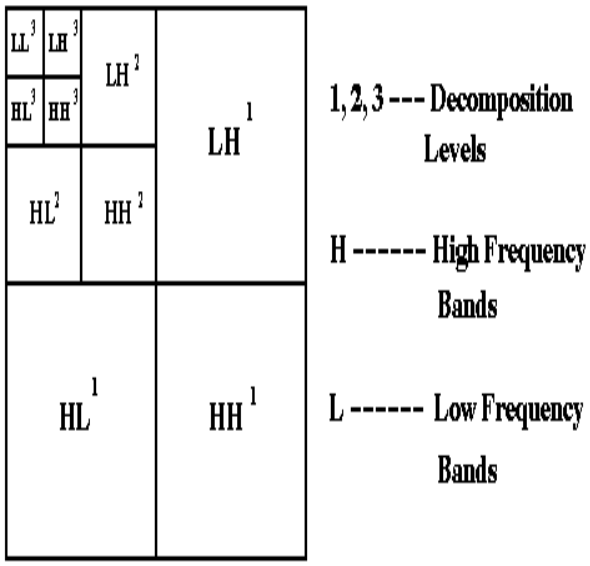

Figure 4 DWT filter up to 3-level

DWT technique of encryption is more efficient than the DCT and DWT, as this technique shows the similarity with the human visual system hence the encryption of data by using technique become easier and HVS is less sensitive to the various bands of the DWT , various bands discussed in the DWT are LH, LL, HL and HH. Embedding of data is easier and allows the increase in robustness of the encryption. Quality of the image remains same even after the encryption has been performed.

Discrete Fourier Transform

Discrete Fourier transformation deals with the dividing the image into the sin and cosine components for the processing. Recurrence group can be easily used for the genuine impairments. Encryption can be easily performed over the using the discrete Fourier transforms. These techniques deal with one or more centre recurrence groups of greatness space of the DFT. Hence it provides the rings of the greatness area.

An opposite Discrete Fourier Transform is performed on the encryptioned size area to remake the advanced information with the implanted encryption [4]

Singular Value Decomposition:

Singular Value Decomposition (SVD) refers to the representation of the data in the form of the matrix. It is the important part in the linear algebra. SVD is basically the technique that works on the matrices that can be altered by using the optimal state of the data.SVD is effiecntly used in the image compression techniques to compress the data of the image. [13]. The SVD of an N x N matrix A is defined by the operation:

$$A = U S V^T$$

Where U and V $\in R^{N \times N}$ are unitary, and S $\in R^{N \times N}$ is a diagonal matrix. Singular values of A are represented by the diagonal entries of the S. are assumed to be arranged in decreasing order $\sigma i > \sigma i +1$. Each singular value σi specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer . In SVD-based encrypting, a frame image is treated as a matrix decomposed into the three matrices; S, U and V^T, as shown below in Figure 5.

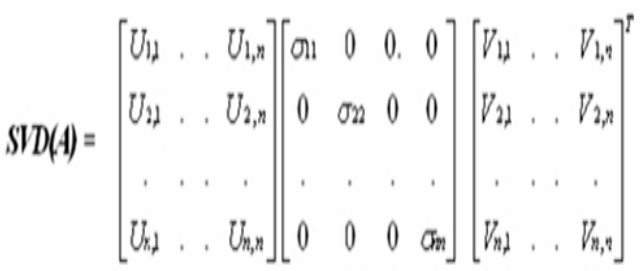

Figure 5: The SVD operation SVD

(A) = U S V T

V. CONCLUSION

Since large amount of data is being transferred over the internet. Security of data to be transferred over the internet is the primary concern of researchers. Copyright of the data is the important to secure the data from the unauthorized access over the internet. Encryption technique acts as the firewall so as to prevent the mischievous elements to access the data. Encryption of image has become the important and challenging area of research. Spatial area is adjusted by adjusting the pixel values. However the encryption by this technique is difficult to optimize. The second domain i.e. frequency domain requires the high computational work for its processing. Various techniques have been survey in this paper, these are singular value decomposition, discrete fourier transform , least bit significance technique, Correlation technique, Discrete wavelet transform, Discrete cosine transform.

Each techniques has its benefits and drawbacks, these are used according to the application for which they are used. Digital Encryption is generally used to provide the authenticity to the signal and may also be used for providing the identity to its owners. Data validation, copyright protection and security of data are provided by the Encryption techniques. Fuzzy logic can also be enhancing the security level by providing high security code with random generation, thus making it more anonymous.

REFERENCES

[1] M. Mohamed Sathik, S.S.Sujatha (2012), 'A Novel based invisible Encrypting Technique for Digital Images', International Arab journal of e-Technology, January 2012, Vol 2,No. 3

[2] Swati Tiwari, R. P. Mahajan (2012), 'A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion', International Journal of Electronics Communication and Computer Engineering, 2012,Volume 3, Issue 1, ISSN 2249 – 071X.

[3] Sangeeta Mishra, Sudhir Sawarkar (2012), 'Image Compression Using Spiht and Neural Network', International Journal Of Computational Engineering Research, November 2012,Vol. 2,Issue. 7, Issn 2250-3005.

[4] Bibi Isac, V. Santhi (2011), 'A Study on Digital Image and Image Encrypting Schemes using Neural Networks', International Journal of Computer

Applications (0975 – 8887), Volume 12– No.9, January 2011

[5] C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake, H. Perez-Meana (2010), 'A Blind Image Encrypting Scheme Robust To Frame Attacks Combined With MPEG2 Compression', Journal of Applied Research and Technology, December 2010, Vol.8 No.3,323-339.

[6] Gaurav Bhatnagar, Balasubramanian Raman (2009), 'A new robust reference encrypting scheme based on DWT-SVD', Computer Standards & Interfaces 31 (2009) 1002–1013

[7] Cheng-Han Yang, Hui-Yu Huang, Wen-Hsing Hsu (2008), 'An adaptive image encrypting technique based on DCT domain', 978-1-4244-2358-3/08 © 2008 IEEE

[8] Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal (2006), 'A Survey on Different Image Encrypting Techniques and Comparative Analysis with Reference to H.264/AVC', 1-4244-0216-6/06, IEEE 2006.

[9] Sakshi Batra, Harpinder Kang Khattra (2013),' An Improved Data Transfer Technique Using Steganography with Encrypting and Visual Cryptography', International Journal of Innovative Technology and Exploring Engineering (IJITEE), , December 2013,Volume-3, Issue-7, ISSN: 2278-3075.

[10] Namita Tiwari, Dr.Madhu Shandilya (2010), 'Evaluation of Various LSB based Methods of Image Steganography on GIF File Format', International Journal of Computer Applications, September 2010, Volume 6– No.2, 0975 – 8887

[11] Snehal V. Patel, Snehal V. Patel (2011), 'Invisible Digital Image Encrypting Using 4-level DWT', National Conference on Recent Trends in Engineering & Technology, 13-14 May 2011, B.V.M. Engineering College, V.V.Nagar, Gujarat, India

[12] Suppat Rungraungsilp, Mahasak Ketcham, Pruch Surakote, Sartid Vongpradhip (2012), 'Data Hiding Method for QR Code Based on Encryption by comparing DCT with DWT Domain', International Conference on Computer and Communication Technologies(ICCCT), May 26-27,2012

[13] Lama Rajab, Tahani Al-Khatib, Ali Al-Haj (2009), 'Image Encrypting Algorithms Using the SVD Transform', European Journal of Scientific Research, ISSN 1450-216X, Vol.30 No.3 (2009), pp.389-401

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301 Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com