International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 1, January- 2013

Analysis Of Encryption And Watermarking Techniques For Secure Bluetooth Transmition Of Image Files

Neha D Parmar
Department of Computer Science & Engineering
Parul Institute of Technology,Gujarat, India

Neha Pandya
Department of Information Technology
Parul institute of Technology, Gujarat, India

Abstract

Encryption and watermarking are complementary lines of defense in protecting multimedia content. Recent watermarking techniques have therefore been developed independent from encryption techniques. This paper focuses mainly on the different kinds of image encryption techniques And the hybrid image protection scheme to establish a relation between the data encryption key and the watermark.

***Keywords*--- Bluetooth security, encryption., Decryption ,watermarking, Robustness, transmission**

1. Introduction

Bluetooth is a type of wireless ad-hoc network. It is also known as Personal area network with IEEE 802.15 standard. Bluetooth technology has many features like low cost, low complexity, low power consumption, ad-hoc in nature. The amount of data to be transmitted is Bluetooth version dependent. Whenever we talk about data transmission through any type of network whether it is LAN, WAN, MAN or PAN the important aspect is how we provide confidentiality in transmitted data.

The information is not only the text, but also audio, vedio, an image and multimedia content. Images have a been widely used in our daily life. However the more extensively we use the images, the more important their security will be. Image security has become an important topic in the current computer world. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the image security. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, multimedia systems, medical imaging, Tele-medicine and military Communication, etc. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues.

Introduction Digital watermarking is the process of embedding or hiding the digital information called watermark into the protected multimedia product such as an image, audio or video. The embedded data can be detected later or extracted from the multimedia for identifying the copyright ownership. Over the past few years digital watermarking has become popular due to its significance in content authentication and legal ownership for digital multimedia data. Digital watermark is a sequence of Digital watermarking technique is one of the solutions to avoid unauthorized copying or tampering of multimedia data. Recently many watermarking schemes have been proposed to address this problem. The watermarking schemes are broadly categories into two main domains i.e. spatial domain and the transform domain. In spatial domain watermarking the watermark is embedded by directly modifying the intensity values of the cover image. The most popular technique is the least significant bit (LSB) method. In transform domain the watermark is embedded by modifying the frequency coefficients of the transformed image. The common methods in the transform domain are Fourier transforms (DFT), discrete cosine transforms (DCT), discrete wavelet transforms (DWT), etc.

CHARACTERISTICS OF WATERMARKING

There are many characteristics that watermarking holds, some of them are as follows:

1. ***Visibility***: an embedded watermark can be either visible or not visible according to the requirement.

2. ***Robustness***: piracy attack or image processing should not affect the embedded watermark. Robustness might also incorporate a great degree of fragility to attacks, i.e. multimedia cover object is totally destroyed if it detects any tapering [10].

3. ***Readability***: A watermark should convey as much information as possible. A watermark should be statistically undetectable. Moreover, retrieval of the digital watermark can be used to identify the ownership and copyright unambiguously.

4. ***Integrity***: No loss of original multimedia carrier.

5. ***Accessibility***: both types of watermarking must permit for accessibility. Visible type allows information handling for any interested entity to call attention to the copy/reproduction rights, while the invisible type necessitates extra authorization information in order to access the watermark.

6. ***Security***: Security: watermarking accounts for the protection of ownership against forgery and unlawful threats. Invisible watermark should be secret and must be undetectable by an unauthorized user in general.
It has been noted that if strong stress is been put on robustness, then invisibility may be weak, however if one puts emphasis on invisibility, then robustness is weak. Therefore, developing invisible and robust watermark is considered as very important issue [11].

2. Research work related to image Encryption Algorithm

The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image data have special properties such as bulk capacity, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique.

2.1. A Scalable Encryption Method, 2012

This method comprises of backward compatibility with the JPEG2000 Images. This encryption technique tells the encrypted images to hold the multilevel encryption method also decreases the computational complexity of the encryption process. In this paper the standard JPEG 2000 decoder is used to decode the encrypted images and some parameters of JPEG 2000 were saved after the encryption process. As the result of this, the duration of the encryption process is controlled by selective encryption algorithms to promote faster processing[7].

2.2. Image Encryption Technique based on the concept of Least Sqare Approximation(LSA), 2012

Mahmood Al-khassaweneh and Selin Aviyente has put forth a novel image encryption technique based on the concept of Least Square Approximation (LSA) .In this paper, the conversion of the original image into the form of encrypted one by the randomly generating vectors. And on the other hand the original image has been decrypted by using the least square approximation concept on the encrypted image and also on the randomly generating vectors. As the result of this, there is a good range of efficiency in this algorithm and also promotes good enhancement in the security aspects[9].

2.3. Enhanced Block based image Encryption Scheame, 2012

Syed Ali Naqi Gilani, M. Ajmal Bangash has developed an enhanced block based image encryption Scheme with Confusion. The authors designed the Block-Based Image Encryption Algorithm (BBIE) which works together with the Blowfish Encryption algorithm. Here the digital image is decomposed into slices, after those two continuous actions that are rotating each 3D true color image slice to 90° which is then follow up by flipping row wise down were done. Also the rendered blocks were then undergo the process of scrambling into the form of converted confused image which is finally follow up by the Blowfish cryptosystem which is actually the process of encryption of the image using a secret key. The result shown that, the correlation between adjacent pixels has been reduced in the entire color component[12].

2.4. Encryption algorithm of enhanced model of AES, 2012

Eyed Hussein Kamala et al have framed an image encryption algorithm of enhanced model of Advanced Encryption Standard. The authors proposed an enhanced model of Advanced Encryption Standard to possess good level of security and better range of image encryption. The modification process can be carried out by adjusting the Shift Row Transformation. As the result shown, that the comparison has been made in between the original AES encryption algorithm and the modified algorithm which produces very good encryption results focusing towards the security against statistical attacks[13].

This technique presents an application of AES (Advanced Encryption Standard) operations in image encryption and decryption. The encrypted cipher images always display the uniformly distributed RGB pixels.
Traditional encryption algorithms such as DES, IDES, are against the text messages to be proposed, which are not suitable for digital image encryption, therefore, an reliable digital image with characteristics is in urgent need of the encryption scheme AES is suitable for image encryption, and decryption with is closely related to some dynamics of its own characteristics.

The Advanced Encryption Standard offers the flexibility of allowing different key sizes 128 bit, 192 bit and 256-bit key and the security is based on the various random key selections, different S-box and strong transformations. Thus the algorithm provides many different flexible implementations. Lastly, this intends to give an insight in understanding the concepts of image cryptography along with the importance of secure image transmission. Apart from that, the paper can be used to be developed further by researchers or programmers and acts as a template for ensuring the protection of image using encryption [22].

2.5. A technique for image encryption using Digital signature

Alok Sinha and Kehar Singh [4] have presented a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the Encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver End, after the decryption of the image, the digital signature can be used to verify the authenticity of the image. In the first step of encryption technique, an error control code is used which is determined in real-time, based on the size of the input image. Without the knowledge of the specific error control code, it is very difficult to obtain the original image. The dimension of

the image also changes due to the added redundancy. This poses an additional difficulty to decrypt the image.

2.6. Lossless image compression and encryption using SCAN

S.S. Maniccam and N.G. Bourbakis [5] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. The drawback of the methodology is that compression encryption takes longer time.

2.7. A new Mirror-like image encryption algorithm and its VLSI architecture

Jiun-In Guo and Jui-Cheng Yen [6] have presented an efficient mirror-like image encryption algorithm. Based on a binary sequence generated from a chaotic system, an image is scrambled according to the algorithm. This algorithm consists of 7 steps. Step- 1 determines a 1-D chaotic system and its initial point $x(0)$ and sets $k = 0$. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates binary sequence from chaotic system Steps-4, 5, 6, and 7 rearrange image pixels using swap function according to the binary Sequence. But this algorithm does not have any compression scheme and authenticity verification.

2.8. A new Chaotic image encryption algorithm

Jui-Cheng Yen and Jiun-In Guo [8] have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image's pixels are rearranged. This algorithm has four steps. Step-1 determines a chaotic system and its initial point $x(0)$, row size M and column size N of the Image f, iteration number no, and constants α, β, and μ used to determine the rotation number. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates the binary sequence. Step-4 includes special functions to rearrange image pixels. But this algorithm does not have any compression scheme and authenticity verification.

2.9. Double image encryption by using Iterative Random Binary encoding in Gyrator Domains

Muhammad Ashfaq Ahmad3 and Shutian Liu have a double image encryption by using random binary encoding and gyrator transform. Two secret images are first regarded as the real part and imaginary part of complex function. Chaotic map is used for obtaining random binary matrix. The real part and imaginary part of complex function are exchanged under the control of random binary data. An iterative structure composed of the random binary encoding method is designed and employed for enhancing the security of encryption algorithm. The parameters in chaotic map and gyrator transform serve as the keys of this encryption scheme. But the encryption method is safer in the comparison with double random phase encoding. But these approaches are generally cumbersome and inconvenient to the user and system. Therefore, there is a need for mechanism/system which can ensure reliable and efficient data security in a convenient way. We focused on these issue and proposing secure image data by using a combination of permutation and encryption technique that solve the image data security problem[23].

2.10. An image encryption approach using a combination of permutation technique

Mohammad Ali Bani Younes and Aman Jantan an Image Encryption Approach presented in aprail 2008 is the combination of permutation technique followed by encryption. They introduced a new permutation Technique based on the combination of image permutation and a Well known encryption algorithm called RijnDael. The original Image was divided into size of 4 pixels × 4 pixels blocks, which were Rearranged into a permuted image using
a permutation process Presented here, and then the generated image was encrypted Using the RijnDael algorithm. The results showed that the Correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved [2].

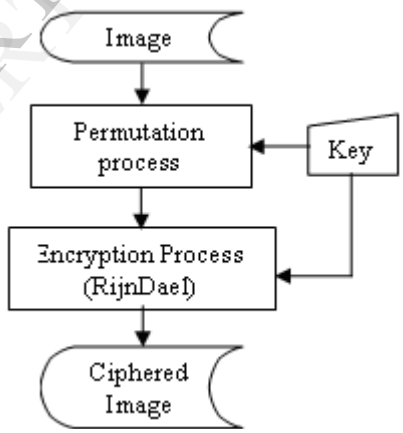

Fig. 1 General block diagram of the permutation technique

But this method has few drawbacks. Like first one , they did not mention the decryption process , second one is , if we are using permutation on block of image than , while sending image to an authorized receiver ,we have to send permutation key too , which is a deep security concern.

2.11. Secure image data by Double Encryption, 2010

secure image data by using a combination of permutation and encryption technique, the aim that image data security should be provided as the top priority of the system. The encryption and decryption of image file data are performed in such a way that making it convenient for the users [1]. The proposed secure image system is designed with the following objective:

Security: confidentiality of data is ensured by use of strong encryption. Image is divided into blocks than permuted and at last gets encrypted then saved to the disk or send onto the network Strong
Access Control: we are using Public-Key Cryptographic Technique, to control the access of the file. This approach enhances the security of file by avoiding unwarranted access.
Transparent Performance: Encrypted file should behave no different from some other files.
Convenience: the system should be convenient to users.

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 neighboring pixels encryption technique will decrease the correlation and increase the entropy of the image. To make a secure image system, the proposed technique divides an age into blocks of n*n size and then perform double encryption process, this will decrease the correlation among neighboring pixels and increase the entropy and transform the block into encrypted form [3].

2.12. A technique for image encryption with combination of pixcel rearrangement scheme based on sorting group vise of RGB-value and explosive inter pixcel displacement, 2012

A new image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption. Experimentally it has shown that pixel rearrangement is enough from image encryption point of view but to send image over open network; inter-pixel displacement algorithm is applied to dispense more armament to image before transmission.

This image encryption method completes in two steps i.e. pixel rearrangement within image using sorting method and in second step image is encrypted using inter- pixel displacement algorithm. For the pixel rearrangement, all the pixels of image are first stored in an array where array sorting is performed. By the sorting method, all the pixels are get compound sort in ascending order of any value i.e. R, G, B and the top we gets 0, 0, 0 pixel if present and 255, 255, 255 in the last position if present. Precedence of sorting is independent of value i.e. R, G, B because the motivation for sorting was reducing the correlation between pixel values. This correlation method by arranging the pixel values in sorting order is better than block shifting as discussed in earlier section.

This array which consists of sorted pixel on basis of RGB value is back transferred to form an image of original length and width size which will then have pixels in ascending order starting from 0, 0, 0 to 255, 255, 255 (both pixel are subject to present in plain image). Now, this image is used for the encryption purpose using the explosive inter-pixel displacement algorithm which has already discussed.

Algorithm for image encryption by using sorting of pixels as per their RGB values and arranging them group-wise which helped to reduce the correlation between pixels and increased entropy value. Experimental results were taken out on Matlab 6.0.1 and this is a lossless image encryption algorithm with results. Histogram of plain image and cipher image is also carried out. Further inter pixel algorithm can be used with another confusing property to result in better image encryption technique. This work can be further extended by using the pyramidal block scheme for image encryption with inter pixel scheme.[14]

3. Research work related to different Watermarking Techniques

Watermarking (data hiding) [15, 16] is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia element for different purposes such as copyright protection, access control, and broadcast monitoring.

3.1. SVD-based watermarking scheme

Although any other watermark embedding and extraction algorithm can be used, we implemented an SVD-based watermarking scheme.
Every real matrix A can be decomposed into a product of 3 matrices $A = U\Sigma VT$, where U and V are orthogonal matrices, $UTU = I$, $VTV = I$, and Σ = diag ($\lambda 1$, $\lambda 2$, ...). The diagonal entries of Σ are called the singular values (SVs) of A, the columns of U are called the left singular vectors of A, and the columns of V are called the right singular vectors of A. This decomposition is known as the *Singular Value Decomposition* of A, and can be written as $T\ UiVi\ ri\ i\ A\ \Sigma = = 1\ \lambda$
where r is the rank of matrix A. Note that each SV specifies the luminance of an image layer while the corresponding
pair of singular vectors specifies the geometry of the image.

The watermarking scheme used in this implementation (or any other SVD-based algorithm) can be primarily used for copyright protection purposes. Watermark extraction requires the value of the scaling factor, the singular values of the Unwatermarked cover image, and the left and right singular vectors of the visual watermark. For different images and Watermarks, this information cannot be stored in receivers with limited storage capacity [17, 18].

3.2. Robust digital water marking technique based on Histogram analysis, 2012

robust digital image watermarking technique that attributes the watermarking process to signal modulation model. It is based on the histogram analysis for maximum intensity value of pixels. First, carrier image is properly segmented into blocks, then the histogram for each block is drawn and the peak frequency of occurrence for intensity moments in the carrier image is identified. Then bit values of

the modulating (watermark) image are used to modulate the histogram peaks of the intensity.

Experimentation and analysis on the proposed algorithm show that it is not only simpler and easier to implement, but also it is very effective, secure and robust against different kinds of attacks such as noise, resizing and rotation. Therefore one can conclude that it establishes a concrete judgment for ownership decision to approve ownership in copy write and ownership disputes.

Testing the proposed algorithm by calculation of the Mean Square Error (MSE) and Peak signal to noise ratio (PSNR) for the modulated images using various attacks such as addition of Gaussian, Poisson, salt & pepper and speckle noise are performed. Moreover, other effects such as inclusion of median filter, resizing and rotating the modulated image are also performed. The obtained results show that the proposed technique is very secure and robust against these attacks but in this technique there is no any authentication [19].

3.3. DWT-SVD based secured image watermarking for copyright protection using visual Cryptography, 2012

a new robust watermarking technique for copyright protection based on Discrete Wavelet Transform and Singular Value Decomposition is proposed. The high frequency sub band of the wavelet decomposed cover image is modified by modifying its singular values. A secret key is generated from the original watermark with the help of visual cryptography to claim the ownership of the image. The ownership of the image can be claimed by superimposing this secret key on the extracted watermark from the watermarked image. The robustness of the technique is tested by applying different attacks and the visual quality of the extracted watermark after applying these attacks is good. Also, the visual quality of the watermarked image is undistinguishable from the original image.

Naor and Shamir had introduced Visual cryptography [20]. in this technique encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two possibilities is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two probabilities is chosen to generate Share1 and Share2. Each share pixel is encoded into two white and two black pixels. Only one cannot give any clue whether the pixel is white or black. The secret image can be revealed only when both the shares are superimposed on each other.

The two major considerations in visual cryptography are pixel expansion and number of shares encoded. If the pixel expansion is smaller then it may results in smaller size of the share. If the multiple secret images are encoded then the same share images requires less overhead while sharing multiple secrets.

In this scheme applied the singular value decomposition along with the Discrete Wavelet Transform. Since the technique utilizes the properties of both DWT and SVD the proposed technique is more robust against different attacks. The innovation of this paper is that the security of the algorithm is increased with the help of visual cryptography on the watermark image. If the second share of the watermark which acts as the key is not present then it is not possible to extract the exact watermark information. It is very difficult to change or remove the watermark without knowing the secret key share as the watermark is split into two shares with random patterns. The Robustness of the technique is justified by giving analysis of the effect of attacks and still we are able to get good visual quality of the embedded watermark [21].

4. Conclusion

In this dynamic & vibrant web world now a days, the security for the digital images has turn out to be exceedingly vital, since the communication by transmission of digital stuffs over the open network occurs very recurrently.This paper includes the survey on the prevailing mechanisms on the encryption techniques & all the watermarking techniques. Encryption techniques are studied & analyzed well to stimulate the performance of the encryption techniques also to safeguard the security proceedings. Watermarking techniques are studied and investigated glowing for copyright protection. To sum up, all the techniques are beneficial for real-time encryption and security persistence. Each encryption & watermarking technique is matchless in its own way, which might be appropriate for diverse applications. Everyday innovative encryption and watermarking technique is sprouting fast to secure. Orthodox encryption techniques will always work out with high rate of security.

With the support of this paper we are approaching up to create one best Hybrid Scheme that integrates both. Encryption Algorithm applied on the superlative watermarking technique. With the help of this Hybrid Scheme we may smear double security protection on the very vital and confidential image data & devoid of any problem we may transmit this confidential image data on network by Bluetooth.

5. 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] Osamu Watanabe, Akiko Nakazaki And Hitoshi Kiya," A Scalable Encryption Method allowing Backward Compatibility with JPEG2000 Images" *IEEE Transactions* pp. 6324-6347,2005.

[8] 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

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

[10] [10] Cox I.J., M.L. Miller, J.M.G. Linnartz, T. Kalker, "A Review of Watermarking Principles and Practices", Digital Signal Processing for Multimedia Systems, K.K. Parhi, T. Nishitani, eds., New York, Marcel Dekker, Inc., PP 461-482, 1999.

[11] [11] Rawat K.S. and D.S. Tomar, "Digital Watermarking Schemes for Authorization against Copying or Piracy of Color Images", Indian Journal of Computer Science and Engineering, Vol.1, PP 295-300, 2010.

[12] Syed Ali Naqi Gilani , M. Ajmal Bangash, "Enhanced Block Based Color Image Encryption Technique with Confusion" *IEEE Transactions* pp. 200-206,2008.

[13] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, "A New Modified Version of Advanced Encryption Standard(AES) Based Algorithm for Image Encryption", *IEEE Transactions on Electronics and Information Engineering,* Vol 1,pp.141-145,2010

[14] Amnesh Goel, Nidhi Chandra," A Technique for image encryption with combination of Pixel rearrangement scheme based on sorting Group vise of RGB value and Explosive Inter Pixel displacement (2012)" Published Online March 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijigsp.2012.02.03.

[15] I. J. Cox, M. L. Miller and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2001.

[16] M. Arnold, M. Schmucker and S. D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*, Artech House, Inc., 2003.

[17] R. Sun, H. Sun, and T. Yao, "A SVD and quantization based semifragile watermarking technique for image authentication," in Proc.Int. Conf. Signal Process., pp. 1592–1595, (2002)

[18] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia 4, 121–128, (2002).

[19] Hamza A. Ali, Sama'a A. K. khamis," Robust digital watermarking technique base on Histogram Analysis (2012)," *World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 163-168, 2012* 163.

[20] Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology– Eurocrypt, pp 1-12, (1995).

[21] Sushila Kamble1, Vikas Maheshkar2 , Suneeta Agarwal3 , Vinay K Srivastava4," DWT-SVD Based secured image watermarking for Copyright protection using visual Cryptography (2012)," Natarajan Meghanathan, et al. (Eds): ITCS, SIP, JSE-2012, CS & IT 04, pp. 143–150, 2012. © CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2113

[22] P. Radhadevi1, P. Kalpana2,"secure image Encryption using AES", IJRET | OCT 2012, Available @ http://www.ijret.org/

[23] Muhammad Ashfaq Ahmad3 and Shutian Liu, Jayant Kushwaha, Bhola Nath Roy," secure image data by double encryption,"double image encryption by using random binary encoding and gyrator transform," *International Journal of Computer Applications (0975 – 8887)Volume 5– No.10, August 2010*