International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

An Efficient Technique for Image Encryption and Decryption for Secured Multimedia Application

Ashish S. Dongare[1], Dr. A. S. Alvi[2], Prof. N. M. Tarbani[3]

[1]Dept. of Computer Science and Engineering,
Prof Ram Meghe institute of Technology and Research, Maharashtra, India.
[23]Professor, Dept. of Computer Science and Engineering,
Prof Ram Meghe institute of Technology and Research, Maharashtra, India.

Abstract - *In the recent years, Internet multimedia applications have become very popular. The rapid growth in the use of multimedia information has made the security of data storage and transmission important in avoiding unlawful, unofficial, unauthorized and illegal use. Encryption is an efficient operation to protect multimedia data secret. There are various techniques which are discovered from time to time to encrypt the images to make images more secure. Moreover, there are many image encryption schemes have been proposed, each one of them has its own strength and weakness. Innovative encryption techniques need to be developed for effective data encryption for financial institutions, e-commerce, and multimedia applications. For future internet applications on wireless networks, cryptographic coding techniques for multimedia applications need to be studied and developed. In this paper, we focus on the efficient encryption techniques for an image in multimedia applications.*

Key Words: **Image Encryption, key Generation, Input Image, LSB.**

1.INTRODUCTION

There has been an explosive growth of using computers, networks, communications and multimedia applications. Multimedia data security is very important for multimedia commerce on the Internet such as video on-demand and real-time video multicast. The image encryption is widely used to secure transmission of data in an open internet works. Every data has its own unique features; therefore different data requires different type of encryption algorithm. Many of the available algorithms are suitable for textual data but they are not suitable for multi-media data such as images, videos. Moreover, traditional cryptographic algorithms which are available for data security are often not fast enough to process the large amount of data generated by different multimedia applications to meet the real-time needs. Because of the increasing demand for information security, image encryption decryption has become an important research area and it has broad application prospects. Image security is of utmost concern as web attacks have become more and more serious. Image encryption decryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication. Since, these images may carry highly confidential information, so these images entail extreme protection when users amass somewhere over an unreliable repository. Furthermore, when people wish to transfer images over an insecure network, then it becomes crucial to provide an absolute protection. In brief, an image requires protection against various security attacks. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), product, financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer.

The primary intention of keeping images protected is to maintain confidentiality, integrity and authenticity. Different techniques are available for making images secure and one technique is encryption. Adopting and applying various encryption algorithms can ensure security of data from spoofing and eavesdropping from the unauthorized attacks and crypto-analyst. However, the current forms of broadcasting and delivery of multimedia data through wireless channels, are highly insecure and vulnerable due to the inherent nature open access from massive users and receivers, if not properly encrypted. Generally, Encryption is a procedure that transforms an image into a cryptic image by using a key. Furthermore, a user can retrieve the initial image by applying a decryption method on the cipher image which is usually a reverse execution of the encryption process. The diverse algorithms are accessible to encrypt information, specifically; RSA, DES, AES, etc.

Cryptography is the study of transmitting secret messages securely from one party to another. It plays an important role to secure confidentiality of data while transferring data particularly via Internet. Within the context of any application-to-application communication, there are some specific security requirements Confidentiality, Authentication, Integrity and Non-repudiation. Cryptography is a method for protecting image-based secrets that has a computation-free decoding process. Now days, the security of digital images has become immensely important in many

applications- medical image, confidential video conferencing, defense database, mobile computing, personal communication etc.

Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption schemes (DES, IDEA, RSA etc.) are not suitable for practical image encryption, especially for image transmission via internet. The main obstacle in designing image encryption algorithms is that it is rather difficult to swiftly shuffle and diffuse data by traditional means of cryptology. In this article, image encryption Technique is proposed which can be used to hide the original image information from an intruder or an unwanted user. The input image may be any standard image format. Cryptography, is the science of secret writing and also the synonym of encryption is the recent area of research. The significance of secret key generation is the backbone of encryption. More works have been carried out for secured digital data transmission than secured image transmission over public networks. In order to protect confidential data or image from intruders, a reliable and efficient encryption / decryption mechanism is desired.

The easiest solution will be to consider an image as a stream of bits and encrypt using conventional algorithms like Data encryption Standard (DES), Advanced Encryption Standard (AES) or International Data Encryption Standard (IDEA) for encryption. However, these schemes do not exploit the unique properties of images like huge data redundancy and no predetermined statistical distribution of pixels. They also require higher computation power and time. The encryption key must be long. Yet, it is difficult to remember it and even storing the key in a database or in a file may be insecure. In addition the protection of the confidentiality of encryption keys is one of the important issues to be dealt with. This issue can be efficiently solved through generating the key before starting the process of encryption/decryption, rather than storing it. The main objective of this study is to increase security in communication by encrypting the information using a key that is created through using an image [10]. Color images are used for key generation. Instead of storing and remembering the secret key we can store the images in the database .

2. LITERATURE REVIEW AND RELATED WORK

Philip P. Dang and Paul M. Chau [1] present a novel scheme, which joint image compression encryption scheme for Internet multimedia applications. The feature of the proposed method includes Discrete Wavelet Transform (DWT) for image compression and Data Encryption Standard (DES) for image encryption. These algorithms allow images can be compressed with high compression ratio and the security of transmission process is enhanced.

Leo Yu Zhang, Yuansheng Liu, Fabio Pareschi, Yushu Zhang, Kwok-Wo Wong, Riccardo Rovatti, and Gianluca Setti [2] under the assumption of plaintext attacks they investigate the security of a classic diffusion mechanism (and of its variants) used as the core cryptographic primitive in some image cryptosystems based on the aforementioned complex dynamic phenomena. They have theoretically found that regardless of the key schedule process, the data complexity for recovering each element of the equivalent secret key from these diffusion mechanisms is only O(1). The proposed analysis is validated by means of numerical examples.

Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani [3] presented a novel algorithm for image encryption based on scan patterns that first shuffle the image completely in two steps and then exploit function XOR. The algorithm trades off between speed and security, so that more complex key which shuffle the image completely results more security but it consume more time. Yet in most complexity mode the algorithm act fast. The proposed algorithm has great performance in terms of sensitivity, speed, and security so that even by a simple key the NPCR, UACI, and Entropy can satisfy security and performance requirements.

Junghwan Kim and Srinvasa R. Basavarasu [4] provide a potential solution to counter one of the shortfalls of data transmission through wireless channel, such as insecurity, by using the AES block cipher operating in stream mode, more specifically the counter mode (CTR). The approach in this work is to use the counter mode to encrypt audio and image data, to show the feasibility of implementation. The simulation results of the application of encryption and decryption confirm the effectiveness of CTR mode for successful reconstruction of audio and image only with the knowledge correct security key.

Naik Riddhi , Nikunj Gamit[5] proposed system focuses on generating keys based on color images. The proposed method is simple and flexible. This method can also be applied on text and video. This prevents the key loss as the users (sender and receiver) don't need to remember their keys. This helps the users store the key securely. It can be generated anywhere using the image and the session. In general, this is a reliable and effective method of cryptography. This provides more security against man-inmiddle attack, brute force attack, compromised key attack and differential attack.

Guodong Ye, Xiaoling Huang [6] presented a novel image encryption algorithm is designed based on auto-blocking and a medical ECG (Electrocardiography) signal. The chaotic Logistic map and generalized Arnold map will be employed. For solving deterministic input problems, the ECG signal and Wolf algorithm are used to generate initial conditions for the chaotic maps. Compared with traditional crypto-architectures, the auto-blocking diffusion operation is performed only in the encryption process. The key stream is generated by a control parameter produced from the plain-image, which is proven to be secure against chosen-plaintext and known plaintext attacks.

Vishakha Kelkar,Hitesh Nemade[7] propose a secured reversible watermarking technique for medical images using Histogram shifting method. They provide extra security to the given watermark with chaos encryption. The given

watermark is encrypted with chaos sequence prior to embedding in the given medical image. Also the block based technique is evaluated for increased watermarking capacity. The results of technique are compared on the basis on MSE and PSNR.

3. THE NEED OF IMAGE ENCRYPTION

Image encryption is necessary for future multimedia Internet applications. Password codes to identify individual users will likely be replaced with biometric images of fingerprints. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper may duplicate or reroute the information. By encrypting these images, the content still has some degree of added security. Furthermore, by encrypting non-critical images as well, an eavesdropper is less likely to be able to distinguish between important and non-important information. Image encryption can also be used to protect privacy. An example for image encryption to protect privacy is in medical imaging applications. Recently, in order to reduce the cost and to improve the service, electronic forms of medical records have been sent over networks from the laboratories to medical centers or to doctors' offices. According to the law, medical records, which include many images, should not be disclosed to any unauthorized persons. Medical images, therefore, should be encrypted before they are sent over networks. Moreover, image encryption can be used to protect intellectual properties. One of concerns of the entertainment industry is that movies and videos in digital format are vulnerable to unauthorized access, theft, and replication. Entertainment industry has lost billion dollars due to the illegal copies. Recently, new technologies have been developed which allows multimedia can be delivered to millions of household very quickly. Entertainment industry will utilize Internet and satellites for multimedia distributions. The threat of unauthorized access during transmission over networks and the threat of illegal copy increase significantly. Image encryption, therefore, can be used to minimize these problems. Although encryption is sufficient to protect digital images and videos in some civil applications, this issues have taken into consideration when advanced encryption algorithms are specially designed for sensitive digital images and videos, for their special features are very different from texts.

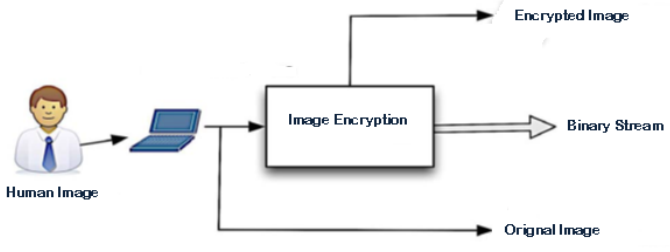

Fig -1: Image Encryption

As show in Fig.1, the first output is sampled from the stream of binary bits, which are packetized. The second output is the encrypted signal. This is due to Applying the Encryption Technique .The third output is sampled directly from the input file. We compare the encrypted signal with the original image sample in the results. We explain the implementation of technique of the encryption and decryption implementation in the following sections.

4. TECHNIQUE FOR ENCRYPTION OF IMAGE

In this technique we propose approach of image encryption with key generation algorithm. Process of encryption is described in given Fig.2 .

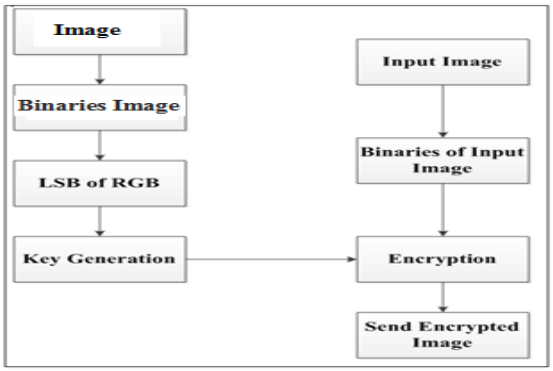

Fig -2: Encryption of Image

A. Binaries Image

It will extract three channels from input image (color image) and converts the values of it to binary values. The binary values are stored in one multidimensional array as Data Here we have to generate total three arrays which represent three different channels of image i.e. red channel, green channel and blue channel.

B. LSB of RGB

In this process we will consider input image for key generation and converts the value of its pixel in binary. After converting in binary; Least Significant Bit (LSB) will considered from each pixel.

C. Key Generation

A cryptographic key is information generated to encrypt and decrypt the message. Generating the cipher image by using key at sender side. At the receiver side the exact reverse is done to getting original image. We will generate keys for encryption/decryption process. In this process consider input image which have to encrypted. For key generation channels (red or green or blue) will be extracted from the selected image. In key generation process three keys are generated from the color image i.e. one key will generated from red channel one key will generated from green and similarly one key will generated from blue channel. After that binary value of each pixel is calculated and these values are stored in one array. After generation of binary array each pixel is scanned and LSB of each pixel is calculated and new

array of these LSB value is generated. Finally, to generate key each bits of LSB array is scanned and neighbor pixels having absolute difference one will be stored in one array.

D. Encryption

After that three different keys will be generated using the image after that using key arrays and arrays of binary value encrypted images are generated. To encrypt the image XOR operation is performed on keys and three different channels of image as shown in Fig.3. In encryption process red channel of input image will be encrypted using the key generated from the red channel of color image which is used for key generation and similarly green channel and blue channels are encrypted with the key generated from the respective channel.

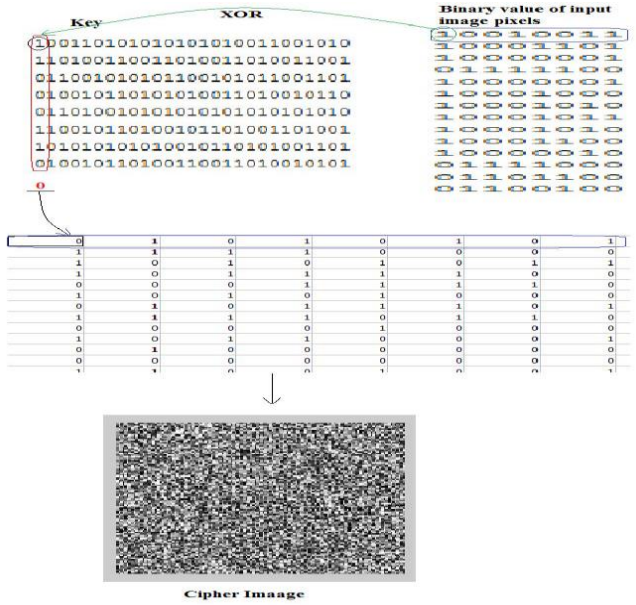

Fig -3: Encryption

E. Decryption

The decryption process is the exact same process as Encryption. For Decryption generating Key by using cipher image hence we don't need to save key which is generated at time of encryption and is efficient as security purpose. After that XOR operation is performed on array of keys and array of cipher images and array of original channel is calculated. This operation is performed on all red, green and blue channels and value of all channels is calculated. After that from the value of all three channels original image is extracted. This process of decryption done on receiver side as describe in Fig.4.

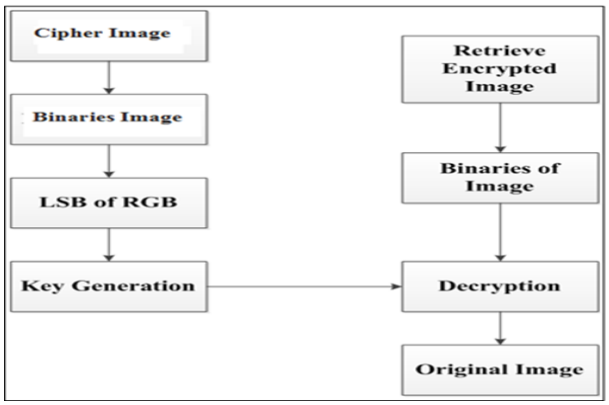

Fig -4: Decryption Process

5. CONCLUSIONS

We analysis the technique which generating keys based on color images. The proposed technique is simple and flexible. This technique can also be applied on text and video. In general, this is a reliable and effective method of cryptography. This provides more security against man-in middle attack, brute force attack, compromised key attack and differential attack. It is a very simple and easy technique for encrypting an image using three different keys will be generated using the image after that using key array and array of binary value encrypted images are generated and performing XOR operation to encrypt/decrypt the image. The proposed technique offers commendable security to color images. This method is suitable for encrypting images of different sizes, types and for different applications

REFERENCES

[1] Philip P. Dang and Paul M. Chau," Image Encryption For Secure Internet Multimedia Applications," *IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, AUGUST 2000.*

[2] Leo Yu Zhang, Yuansheng Liu, Fabio Pareschi, Yushu Zhang, Kwok-Wo Wong, Riccardo Rovatti, and Gianluca Setti," On the Security of a Class of Diffusion Mechanisms for Image Encryption," *IEEE Transactions On Cybernetics ,Volume: PP, Issue: 99 ,March 2017.*

[3] Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani," A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR," *International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.6, No.5 (2013), pp.275-290.*

[4] Junghwan Kim and Srinvasa R. Basavarasu," On The Voice And Image Data Encryption Using Advanced Encryption Standard (AES) In Counter Mode For Multimedia Broadcasting," *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2015.*

[5] Naik Riddhi , Nikunj Gamit," An Efficient Algorithm for Dynamic Key Generation for Image Encryption," *IEEE International Conference on Computer, Communication and Control (IC4-2015).*

[6] Guodong Ye, Xiaoling Huang," An image encryption algorithm based on auto-blocking and ECG signal," *IEEE MultiMedia,Volume: 23, Issue: 2, Apr.-June 2016.*

[7] Vishakha Kelkar, Hitesh Nemade," Reversible Watermarking in Medical Images Using Histogram Shifting Method with Improved Security and Embedding Capacity," *IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), May 2016*.

[8] Mohit Kumar, Akshat Aggarwal, Ankit Garg," A Review on Various Digital Image Encryption Techniques and Security Criteria," *International Journal of Computer Applications (0975 – 8887)Volume 96– No.13, June* 2014.

[9] Abul Hasnat, Dibyendu Barman, Satyendra Nath Mandal," A Novel Image Encryption Algorithm Using Pixel Shuffling and Pixel Intensity Reversal," *International Conference on Emerging Technological Trends (ICETT), Oct. 2016*.

[10] Aarti Soni, Suyash Agrawal, "Using Genetic Algorithm for Symmetric Key Generation in Image Encryption", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),Volume 1, Issue 10, December 2012.*