ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

A survey on image cryptography and their techniques

Manisha Solanki, Mahendra K Verma

***Abstract*—images are the set of values that are distributed in a vector which represents the real world objects. Therefore sometime these images are much sensitive and contain private and essential information. The security of such data is a need of computational and security. In this paper image cryptography and their recent development are investigated. In addition of that a new crypto graphic technique is proposed to enhance the traditional approach of image cryptography. Therefore the paper includes the survey about the image and image encryption techniques additionally a new technique that is proposed in order to enhance the cryptographic security in image data.**

***Keywords*—** image, image cryptography, data security, network security, survey

I. INTRODUCTION

After discovery of computer, data becomes much sensitive and essential in our daily life. A number of users continuously generate data for different purposes. Some of data among these is much sensitive and confidentialtherefore security is a primary aspect of computer data security. The art of preserving information by transforming it into an unreadable format, called cipher text only those who possess a secret key can decipher the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking, although modern cryptography techniques are virtually unbreakable.

As Internet and other communication technique become more dominant, electronic security is becoming increasingly important. Cryptography is used in various applications such as e-mail, credit card, and other data. Cryptography systems can be broadly classified into symmetric-key that use a single key for both sender and recipient, and public-key that use two keys, a public key known to everyone and a private key that only recipient of messages can use [1].

There are a number of applications available by which private and sensitive data is transmitted in untrusted network. Basically most of the time user sends data from a trusted network to a trusted network but between source and target network remains unsecure. Therefore, the applications are utilizes the cryptographic techniques to providing security and confidentiality. In this paper the main aim is to find the efficient and optimum solution for color image cryptography. Efficiency concerned with minimizing the computational resources in terms of memory and execution time. Thus the desired cryptographic system required to work in less resource consumption. In order to develop such approach simple mathematical techniques and lightweight cryptographic standards are required to employ.

This section provides the basic aim and overview of the proposed study. In the next section first of all required to understand the image and their basic concepts.

II. BACKGROUND

This section describes the basics of different techniques and technology that are used to understand the image and their cryptographic manner.

A. Digital Image

A digital image or image is a computer generated picture that appears on-screen. In terms of image processing that is representable with a 2D array or vector. These array are contains some values, known as pixels, pixel values are varying between 0-255. By using combination of these values real world information is stored. One way to describe an image using numbers is to declare its contents using position and size of geometric forms and shapes like lines, curves and circles [2].

A vector image is resolution independent, means you can enlarge or shrink image without affecting output. Vector images are preferred way to represent many illustrations. Bitmap or raster images are “digital photographs” they are most common form to represent natural images. The term bitmap refers to how a given pattern of bits in a pixel maps to a specific color.A bitmap images is an array, where value of each element called a pixel correspond to color of that portion. Each horizontal line in image is called a scan line. The values in matrix depict brightness of pixels. Larger values correspond to brighter areas and lower values are darker [2].

B. Cryptography

There are various different kinds of cryptographic schemes are available.Based on nature of Encryption algorithms can be classified into two broad categories- Symmetric and

Asymmetric key encryption sometimes an additional approach is used that is known as the hybrid encryption algorithms [3].

Symmetric Encryption

Symmetric encryption is classical technique of encryption. A secret keysuch as a number or word of random letters can beused to change content of the text documents. This might be as simple as shifting each letter by a number of places. As long as both sender and recipient know secret keyand can encrypt and decrypt messages.

Asymmetric Encryption

The problem with secret keys is exchanging them over Internet while preventing them from attackers. Anyone who know secret key can decrypt message. One answer is asymmetric encryption.There are two related keys or a key pair. A public key is made for anyone who want to send a message. Second a private key is that only know by the receiver. Any message that is encrypted by using public key can only be decrypted by applying same algorithm, but by matching private key. This means that you do not need to worry about passing public keys over Internet. A problem with asymmetric encryption is that, it is slower than symmetric encryption.

Hybrid Cryptography

Symmetric and asymmetric ciphers each have their own advantages and disadvantages. Symmetric ciphers are significantly faster than asymmetric ciphers but require sharing secret keys. The asymmetric algorithms allow public key and key exchange systems. So a hybrid cryptosystem is protocol to combine specific advantages of two encryption methods – speed and security [4].

C. Image encryption

A digital image can be a two dimensional array. The elements of this array are referred as pixels. Every pixel carries an intensity value and a location. Therefore, it is essential to verify integrity, confidentiality and authenticity of transmitted digital images over network. One of the significant known solutions that secure data against unauthorized access or hackers is encryption. The procedure of encryption converts plain-data into cipher through an algorithm with one or more keys.

Image encryption algorithms attempt to convert original images to other image that are difficult to understand to keep confidentiality between users. It is important that without a key for decryption, nobody could get the content. Majority of algorithms are used for encryption. However they do not fit for multimedia data [5].Image encryption algorithms can be categorized into full encryption and partial encryption based on the sum of encrypted data or according to the percentage of the encrypted data.The time for processing of encryption and decryption is the main concern in real-time image communication. Time can be categorized into two levels, one for encryption time and another for time for transferring images. The first step is to choose a robust, fast and easy method to implement to reduce time. Encryption and decryption algorithms are not fast enough to deal with significant amount of transmitted data. A significant criteria relating to method is to decrease image encryption size and maintain quality of image. Partial Encryption is a suitable method to encrypt only the lowest portion of data to lessen the computational requirements of enormous amounts of multimedia data. It is essential to lessen the images encryption time in distributed network by minimizing the sum of data to encrypt and attaining a reasonable security and minimizing the computation.

On the other hand, the traditional full encryption algorithms are used to completely encrypt an image and treat all bits similarly.It has greater computational complexity than partial encryption. Furthermore, it takes more time in comparison with partial encryption. Therefore, multimedia data needs either a full or selective encryption according to requirements of the application. For instance, applications of military and law enforcement need full encryption. Nevertheless, there is a range of spectrum applications that require lower security levels, as in medical images that are attained by partial encryption.

III. LITERATURE STUDY

This section provides the studies that are recently made to develop an efficient and robust algorithm.

Cryptography is a technique in which security in communication overnetwork is provided. Using Cryptography technique information is converted intounreadable form. Multimedia data contain different types of datathat include text, audio, video, graphic, images. ***MahfuzulhoqChowdhury et al [6]***provide an initiation of an technique for multiple selective region image cryptography based on both RC4 stream cipherand chaos. This approach is derived from the standard RC4 algorithm. But Currently RC4 isvulnerable. So for making image encryption technique more secure, they proposed RC4with chaos. And shows that proposed method boost image security over network with several types of attack.

Deepak Pant et al [7] propos a novel confusion and diffusion algorithm for image encryption based on logistic map and cheat image. They choose initial condition and control parameter of logistic map as secret key. The cheat image selected from most common images in public network, together with chaotic matrices generated by logistic maps, is employed both in encryption and decryption processes to encrypt and recover the plain image. One cheat image can be used to encrypt a great number of plain images if the cheat image does not attract the attention of the attackers. The computer experiments such as statistical analysis, sensitivity analysis, differential attack analysis and cheat characteristic analysis, prove that proposed image encryption algorithm is robust and secure enough to be used in practical communication.

T. Karthik et al [8] studied about the network optimization technique and provide their contribution as Network

Optimization techniques are generally used data transfer quickly without loss. Network Optimizationis also applied on power consumption of network. Thus efficient network system concentrates onPower Utilization, Deadlock Lock avoidance and Error Recovery process. Network consists of various nodes that used Power. To manage the Power Consumption in the network, LinkNode Heuristic Algorithm is applied as the optimization technique. The Algorithms work with the optimization modulethat nodes are not used for particular time, means switched to idle state. When the node becomes active to transferthe data then it is changed to awaken state. During data transmission, router is set all node values either on or off. In proposed module efficient power consumption network is focused only on energy utilization. During the data transfer some packets is dropped. This ARS technique is mainly focused on error recovery and to avoid deadlock.Every node is maintained and monitored by Router. If the data transmission is takes place for senderand receiver means router allocates the path, make the nodes available and rest of nodes make in disabled state.

In digital word security is a most important issueand data hiding with image cryptography is one of thepossible ways to ensure the security of the importantmessage from outer world. In this paper we proposed anovel technique that encrypted the message such a ways thatthe message encoded as well as hidden in an image. ***Manoj Mukherjee et al [9]***proposed solution is to use image cryptography to hidetextual message. The proposed technique use of anencryption technique that is based on Fibonacci series &image encryption and a secret key generated from theimage.

The chaotic cryptography is gaining more attention than others becauseof its lower mathematical complexity & better Security. It also avoidsthe data spreading hence reduces the transmission cost & delay. Thedigital image cryptography which is based on chaotic systems utilizesthe discrete non-linear system dynamics generally called chaotic maps.Depending upon the type of system many types of chaotic maps areavailable. By combining them a large number of cryptographictechniques could be designed. In this paper ***Lalita Gupta et al [10]***presents a "Fast EfficientLow Complexity Image Encryption Technique" in the proposedtechnique; confusion and diffusion applied hence the encryption can beachieved quickly. Also the diffusion template is created by randomnumber generator based on Gaussian distribution. The technique usesBakers map and capable of providing the key length of 64 bitsalthough it's length can be extended further.

This section involves the different techniques and methods that are obtained to improve the color image cryptography.

IV. PROPOSED WORK

Due to search of efficient and effective cryptographic approach for image, various techniques are found. There are some key problems are discussed in image cryptographic approach.

1. Color image and their sensitive information are distorted when color images are used. In other words color information's are not preserved during encryption and decryption process.
2. Most of the methods are utilized the substitution and sharing based techniques in order to encrypt images, during man in middle attack and DoS attack this kind of information easily spoofed by attacker.
3. Recovery and cryptography consumes more time: the images of high quality required more time for encryption and decryption of images.

Therefore a suitable, secure and efficient technique is required for improving the process of image cryptography.

To overcome the image cryptographic process a new hybrid approach is used for encrypts and decrypts the images. To overcome the above given problems, which are directly or indirectly a kind of MAN in middle attack. Therefore a hybrid cryptographic approach is proposed for securing the Bluetooth communication. The proposed hybrid cryptographic technique is based on triple DES and tiger algorithm. Using the given approach the data is unrecoverable if data is stolen between the communications.

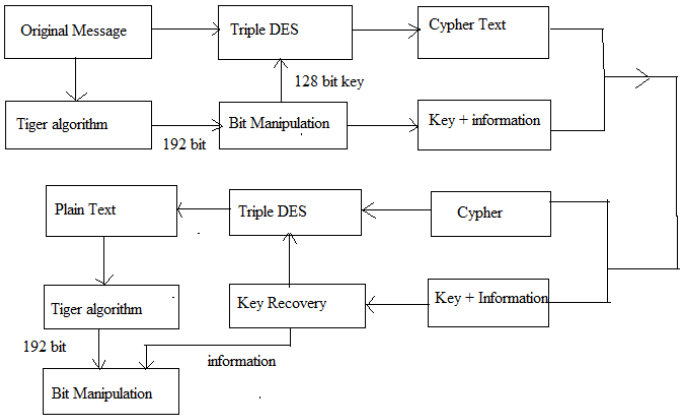

Figure 1 proposed system

the proposed system is given using the figure 1 where plain text is first produced over triple tiger algorithm by which 192 bit hash key is generated, this key is given as input to the bit manipulation phase, where 192 is divided into 3 X 64 bit blocks, here a random process is called and one of the part is discarded. Hence 128 bit key and discarded part as information is preserved for future use. The obtained 128 bit key is further used in triple DES algorithm with text to encrypt file after encrypted file as cypher text, discarded part information and 128 bit key is sent over network. At the receiver end message is recovered in form of cypher text, discarded part information and 128 bit key. 128 bit key is used as key for decrypting the text, and for validation of original message tiger is again utilized for generating 192 bit hash and using information file 128 bit is recovered for similarity matching.

V. CONCLUSION

The security is essential need for computational domain for both network as well as data. In this presented work the image cryptography is taken as investigation domain. The image cryptography is sometimes different from the traditional cryptographic techniques. Thus a survey on different existing techniques and recently developed technique is provided in this paper. During observation of the recently proposed techniques most of the work is performed for the performance enhancement of the encryption and decryption time. Thus finally a new hybrid solution for image cryptography is proposed and explained. The proposed technique is promising to perform the encryption efficiently with less resource consumption. In near future the proposed approach is implemented using the JAVA technology and their performance results are demonstrated.

REFERENCES

[1] VeerrajuGampala, SrilakshmiInuganti, SatishMuppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[2] Clerk Maxwell, "Digital image representation", http://pippin.gimp.org/image_processing/chap_dir.htm

[3] Sian-Jheng Lin and Wei-Ho Chung, Member, IEEE, "A Probabilistic Model of Visual Cryptography Scheme With Dynamic Group", IEEE Transactions On Information Forensics And Security, Vol.7, No.1, February 2012

[4] SankalpPrakash, MridulaPurohit, "Applied Hybrid Cryptography in Key-pair Generation of RSA implementation", Applied Hybrid Cryptography in Key-pair Generation of RSA implementation IJICCT–JUL 2013;Vol 1,Issue 1;ISSN 2347-7202

[5] Lahieb Mohammed Jawad and Ghazali Bin Sulong, "A REVIEW OF COLOR IMAGE ENCRYPTION TECHNIQUES", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1, November 2013

[6] MahfuzulhoqChowdhury, Md. Moniruzzaman and ParijatPrashunPurohit, "Multiple Selective Regions Image Cryptography on Modified RC4 Stream Cipher", International Journal of Grid Distribution Computing Vol.7, no.3 (2014), pp.189-198

[7] Deepak Pant, ManishMadhavTripathi, Ms. SonaliYadav, "Architectural Framework of Image Cryptography By Hybrid Approach of Logistic Map and Cheat Image", International Journal of Engineering Technology Science and Research ,Volume 2 Issue 3 March 2015

[8] T. Karthik and K. Rajkumar, "Efficient Power Management and Data Intensive Computer Systems in Computer Networks", Indian Journal of Science and Technology, Vol 8(12), 64835, June 2015

[9] Manoj Mukherjee and DebabrataSamanta, "Fibonacci Based Text Hiding Using ImageCryptography", Lecture Notes on Information Theory Vol. 2, No. 2, June 2014

[10] Lalita Gupta, Rahul Gupta and Manoj Sharma, "Low Complexity Efficient Image Encryption TechniqueBased on Chaotic Map", International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 11 (2014), pp. 1029-1034