ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

A Review: Image Encryption with RSA and RGB randomized Histograms

Gajendra Singh Chandel [1], Pragna Patel [2]

Assistant Professor, Computer Science and Information Technology Department, SSSIT, Sehore[1]

M.Tech Research Scholar, Computer Science and Information Technology Department, SSSIT, Sehore[2]

Abstract*:* In this paper we discuss and survey several aspects of Image Encryption and Decryption. In today's era it is a crucial concern that proper encryption decryption should be applied so that unauthorized access can be prevented. For this we will survey related researches and done some problem identification. Based on our survey we suggest some future suggestion which can be useful for image encryption.

Keywords: Image Encryption, Chaos, DES, Security Measures

1. INTRODUCTION

In [1] author suggested that Encryption and decryption of original message is based on key value [1]. Very few algorithms like RSA, Quadratic residuosity, Phi-hiding assumption, etc. provides computational hardness [2] and it makes difficult to break a key by an adversary whose objective is to find the original message. Crux of cryptography was arrived in behalf of Loam Battle I to protect information from cryptanalyst. In this day, facts capture recognize in internet is assuming, hence we attempt to ensure the secure data transfer.
In addition, every cryptographic algorithm must satisfy the execution time and high level security channel according to selection of Advanced Encryption Standard (AES) [3].

In [4] author suggest that However, employing encryption in relay based cooperative wireless communication results in multiple drawbacks. First: encryption requires an extra-large amount of bandwidth because of the added overhead packets. Second: the performance deteriorates extensively due to the avalanche effect [5][6] in wireless fading channels, which tremendously reduces the effective bandwidth utilization. This is in addition to the delay caused by the processing time required by the encryption and decryption algorithms at the source and destination sides, respectively. At present, according to its own characteristics of the images, there are many encryption algorithms have been proposed [7]-[13]. Viewing from the point of transform domain they are divided into time-domain encryption and frequency domain encryption.

The remaining of this paper is organized as follows. In Section 2 Literature Survey. In section 3 we discuss about the problem domain. Analysis is given in section 4 the conclusions and future directions are given in Section 5. Finally references are given.

2. LITERATURE SURVEY

In 2003, Sinha [14] proposed a technique to encrypt an image for secure transmission using the digital signature of the image. Digital signatures enable the recipient of a message to authenticate the sender of a message and verify that the message is intact.

In 2004, Shujun Li et al. [15] have pointed out that all permutation-only image ciphers were insecure against known/chosen-plaintext attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images.

In 2005,Zhi-Hong Guan et al. [16] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image.

In 2006, Mitra A et al. [17] have proposed a random combinational image encryption approach with bit, pixel and block permutations. The main idea behind their work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits,pixels and blocks using certain permutation techniques. From the results, it is observed that the permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation.

In 2012, Long Baoa et al. [18] proposed chaotic system shows excellent chaotic behaviors. To demonstrate its

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

application in image processing, a new image encryption scheme using the proposed chaotic system is also introduced. Computer simulation and security analysis demonstrate that the proposed image encryption scheme shows excellent encryption performance, high sensitivity to the security keys, and a sufficiently large key space to resist the brute attack. But in this paper random like nature of chaos is not considered.

In 2012, Ahmad Abusukhon et al. [19] suggested that in cryptographic application, the data sent to a remote host are encrypted first at the source machine using an encryption key then the encrypted data are sent to the destination machine. This way the attacker will not have the encryption key which is required to get the original data and thus the hacker will be unable to do anything with the session. They propose a novel method for data encryption and our method is based on the transformation of a text file into an image file on both client and server machines. They analyze our algorithm by calculating the number of all possible key permutations.

In 2012, Anal Paul et al. [20] suggest that some chaos based algorithms are working well and resists many type of crypto analysis attacks, but it takes lot of time for encryption and decryption. Some of chaos based algorithms are very fast but their strength to resist attack is questionable. So these have motivated us to design a crypto system which will take less amount of time for encryption and decryption and it should resist all type of crypto analysis attacks. They have developed an advanced image encryption scheme by using block based randomization and chaos system. Here we discuss a block based transformation algorithm in which image is divided in to number of blocks. Then these blocks are transformed before going through a chaos based encryption process. At the receiver side after decryption, these blocks are re- transformed in to their original position. The main advantage of this approach is that it reproduces the original image with no loss of information during the encryption and decryption process in a reasonable amount of time, and due to sensitive chaos system becomes it more secure and reliable over the network.

In 2012, Vinay et al. [21] presents securing the transmission of medical images. The presented algorithms will be applied to images. Their work presents a new method that combines image cryptography, data hiding and Steganography technique for denoised and safe image transmission purpose. In This method they encrypt the original image with two shares mechanism encryption algorithm then embed the encrypted image with patient information by using lossless data embedding technique with data hiding method after that for more security. They apply steganography by encrypted image of any other medical image as cover image and embedded images as secrete image with the private key. In receiver side when the message is arrived then they apply the inverse methods in reverse order to get the original image and patient information and to remove noise we extract the image before the decryption of message.

In 2012, Anoop B N et al. [22] proposes a system of secure image transcoder which mainly focuses on multimedia applications such as web browsing through mobile phones, in order to improve their delivery to client devices with wide range of communication, storage and display capabilities. Their system based on CKBA encryption ensures end to end security. The performance of the system has been evaluated for different images.

In 2013, Neha Chauhan et al. [23] proposes region-adaptive watermarking algorithm which will be used for the novel application to detect watermark attacks. The major advantages of the proposed watermarking detection technique are PSNR and RGB Intensity value. For tamper detection using linear classifier by providing these discriminating features. The watermark is embedded on different regions of the host image using a combination of discrete wavelet transform and singular value decomposition technique. Certain types of attack have occurred and there is a novel use the region-adaptive watermarking technique as a means to detect. At the same time,
translation, scaling and rotation belongs to geometric attacks are also applied. The severity of these attacks can be adjusted by modifying their corresponding parameter values.

In 2013, Mohammad Ashiqur Rahman et al. [24] suggest that the risk analysis is an important process for enforcing and strengthening efficient and effective security. Due to the significant growth of the Internet, application services, and associated security attacks, information professionals face challenges in assessing risk of their networks. The assessment of risk may vary with the enterprise's requirements. Hence, a generic risk analysis technique is suitable. Moreover, configuring a network with correct security policy is a difficult problem. The assessment of risk aids in realizing necessary security policy. Risk is a function of security threat and impact. Security threats depend on the traffic reachability. Security devices like firewalls are used to selectively allow or deny traffic. However, the connection between the network risk and the security policy is not easy to establish. A small modification in the network topology or in the security policy, can change the risk significantly. It is hard to manually follow a systematic process for configuring the network towards security hardening. Hence, an automatic generation of proper security controls, e.g., firewall rules and host placements in the network topology, is crucial to keep the overall security risk low. They first present a declarative model for the qualitative risk analysis. They consider transitive reachability, i.e., reachability considering one or more intermediate hosts, in order to compute exposure of vulnerabilities. Next, we formalize our

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

risk analysis model and the security requirements as a constraint satisfaction problem using the satisfiability modulo theories (SMT). A solution to the problem synthesizes necessary firewall policies and host placements. They also evaluate the scalability of the proposed risk analysis technique as well as the synthesis model.

In 2013, Manoj Kumar Ramaiya et al. [25] suggested that Image steganography is a technique for hiding information into a cover image. Least Significant-Bit (LSB) based approach is most common steganographic technique in spatial domain due to its easiness and hiding capacity. All of existing methods of steganography focus on the embedding strategy with less concern to the pre-processing, such as encryption of secrete image. The conventional algorithm does not provide the preprocessing required in image based steganography for better security, as they do not offer flexibility, robustness and high level of security. Their proposed work presents a unique technique for Image steganography based on the Data Encryption Standard (DES) using 64 bit block size of plaintext & 56 bits of Secrete key. The preprocessing provide high level of security as extraction of image is not possible without the knowledge of mapping rules of S –Box and secrete key of the function.

In 2013, Praloy Shankar De et al. [26] attempt has been made to focus on an algorithm of cryptography that was made by using old methodologies. DEDD Symmetric-key cryptosystem is the new approach to symmetric key algorithm. By this method they can doubly encrypt and doubly decrypt the message. It means the sender will generate the cipher text from the plain text twice. The receiver will also have to decrypt the ciphers for two times and then the communication between them will be completed. For generating the key, they will take the message length in first encryption and in second encryption
they will apply shifting technique.

In 2013, Seetaiah Kilaru et al. [27] suggest that security is the main concern in any field. With the
frequent attacks, it is a big challenge for the users to protect the digital images which are transmitting over internet. Singular Value Decomposition (SVD) provides a solution up to a greater extent. Author suggests that by using the Wavelets, invisible watermark embed into the original watermark. The main focus concentrated on the wireless communications; hence it is important to consider some factors into consideration, they are size of an image and requirements of bandwidth. Keeping in view of all these parameters, compression and transmission should be done. The proposed algorithm uses the SVD method along with compression. The proposed algorithm is robust against all common attacks which exist in image processing field. Tests have been done and results are satisfactory in terms of imperceptibility and security.

3. RSA ALGORITHM

The key terminology as given in [28]:

Plaintext (Clear text)
The intelligible message which will be converted into an unintelligible (encrypted) message

Cipher text
A message in encrypted form

Encryption
The process of converting a plaintext message into a cipher text message

Decryption
The process of converting a cipher text message into a plaintext message

Key
A parameter used in the encryption and decryption process.

Cryptosystem
A system to encrypt and decrypt information

Symmetric Cryptosystem
A cryptosystem that uses the same key to encrypt and decrypt information

Asymmetric Cryptosystem
A cryptosystem that uses one key to encrypt and a different key to decrypt

Cryptography
The use of cryptosystems to maintain the confidentiality of information

The Rivest-Shamir-Adleman (RSA) algorithms is one of the most popular and secure public-key encryption methods [29]. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.
Using an encryption key (*e*,*n*), the algorithm is as follows:

1. Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.

2. Encrypt the message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.

3. To decrypt ciphertext message C, raise it to another power *d* modulo *n*

The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user.

How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as *p* and *q*.

2. Set *n* equal to *p* * *q*.

3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1

4. Find *e* such that *e* * *d* = 1 (**mod** ((*p*-1) * (*q*-1)))

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

4. PROBLEM DOMAIN

After discussing several research works we can come with some problem area in the traditional approaches which are following:

1) There are several research work is done in the image encryption and decryption, but there is the need of RGB(Red, Green and Blue) randomization so that information loss is reduced.
2) There is the need of DES, RSA algorithm to be used for image encryption and decryption[30]. We can apply DES and RSA algorithm so that the size of key spaces can be increased and attacking by the brute force technique is weak.
3) The algorithm must support color histograms with logical key space.
4) Image XOR can be performed for making more powerful encryption.
5) Clustering and Fuzzification is also used for providing more impact on encryption.
6) It can be applied on Network Communication for sending encrypted images. So it can be useful in the military services.

5. ANALYSIS

After studying and observing several research works we compare the result discussions by their techniques, so that we identify the good and flaws presented in the previous research.

S.no	Approach	Information Accuracy	Information accuracy after Encryption
1	SPN structure [18]	Leena Image 7.5534	7.9669
2	SPN structure [18]	Circle Image 6.0408	7.9652
3	SPN structure [18]	Clock Image 6.7057	7.9667
4	PSNR Comparision [27]	Clown Image 39.43	Clown Image 32.52
5	PSNR Comparision [27]	Couple Image 39.57 9	Couple Image 30.69
6	Block Based Transformation [24]	0.0063	5.4402
7	Block Based Transformation [24]	0.0049	5.5286
8	Block Based Transformation [24]	0.0044	5.5407

6. CONCLUSION

In this paper we survey and analyze several image encryption and decryption techniques. On the basis of our study we find the problem formulation as well as analysis. So our study analyses and also provide future enhancement directions. Based on the above study we provide the following future directions which can be helpful in better detection:

1) We can use Powerful encryption technique like DES and RSA.
2) Need of Increasing RGB randomization and security key randomization for improving image security.
3) We can improve the block size or bit encryption standard like 128 bit and 256 bit.
4) Chaos-based ciphers should not be susceptible to traditional differential and linear cryptanalysis attacks so hybridization is the better possibility.

REFERENCES

[1] D. Rajavel, S. P. Shantharajah," Cubical Key Generation and Encryption Algorithm Based on Hybrid Cube's Rotation", Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012.
[2] Stallings William, "Stalling Cryptography And Network Security", 4/E – 2006 Pearson Education, Inc.
[3] Michael R. Garey and David S. Johnson, "Computers and Intractability: A Guide to the Theory of NP-Completeness", W.H. Freeman (1979).
[4] National Institute of Standards (NIST): FIPS Pub 197: Advanced Encryption Standard AES (2001).
[5] Li Qian. Study on Color Image Encryption Algorithms Based on Scan Methodology And Chaotic Sequence. Computer Application and Software, 2008,25(7):237..239.
[6] Liu Lijun. Image Encryption Algorithm Based on New Composite Chaotic Sequences.Computer and Digital Engineering, 2008,36(1):90 ..94.
[7] Li Peng.Image Encryption Algorithm Based on Super-Chaotic Sequences. Microelectronics and Computer, 2008, 25(3).
[8] Gao Jie.New Chaotic Image Encryption Algorithm Based on Hybrid Feedback. Computer Application, 2008,28(2):434..436.
[9] Chen G R,Mao Y B,Chui C K.A symmetric image encryption scheme based on 3D chaotic cat maps[J].Chaos Solution and Frctals,2004,21:749-761.
[10] Lv Feng. Informatics and Coding. The People's Posts and Telecommunications Press,2005.
[11] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol[M]. Peking: Tsinghua University Pres, 2007.
[12] Suri , P. R . ; Rani , S. Bluetooth security Need to increase the efficiency in pairing [J]. IEEE/ Southeastcon , 2008.
[13] Fengying Wang. Dynamic Key 3DES Algorithm of Discrete System Based on Multi-dimension Chaos[J]. Microelectronics and Computer, 2005, 7: 25-28.
[14] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Source: Optics Communications, vol.218, no. 4, 2003.
[15] Li. Shujun, Li. Chengqing, C. Guanrong, Fellow., IEEE., Dan Zhang., and Nikolaos,G., Bourbakis Fellow., IEEE. "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004.
[16] G. Zhi-Hong, H. Fangjun, and G . Wen ie , "Ch aos - based image encryption algorithm,"Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.
[17] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science,vol. 1, no. 1, p.127, 2006.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

[18] Long Bao, Yicong Zhou,C. L. Philip Chen," A New Chaotic System for Image Encryption", 2012 International Conference on System Science and Engineering June 30-July 2, 2012, Dalian, China.
[19] Ahmad Abusukhon and Mohammad Talib, "A Novel Network Security Algorithm Based on Private Key Encryption", IEEE 2012.
[20] Anal Paul, Nibaran Das and Agyan Kumar Prusty, "An Advanced Gray Image Encryption Scheme by Using Discrete Logarithm with Logistic and HEH64 Chaotic Functions", IEEE 2012.
[21] Vinay Pandey, Manish Shrivastava, "Medical Image Protection using steganography by crypto-image as cover image", International Journal of Advanced Computer Research (IJACR) Volume-2 Number-3 Issue-5 September-2012.
[22] Anoop B N, Sudhish N George , Deepthi P P," Secure Image Transcoding technique using chaotic key based algorithm", International Journal of Advanced Computer Research (IJACR),Volume-2 Number-4 Issue-6 December-2012.
[23] Neha Chauhan, Akhilesh A. Waoo, P. S. Patheja," Attack Detection in Watermarked Images with PSNR and RGB Intensity" ,International Journal of Advanced Computer Research (IJACR),Volume-3 Number-1 Issue-9 March-2013.
[24] Mohammad Ashiqur Rahman and Ehab Al-Shaer, "A Formal Approach for Network Security Management Based on Qualitative Risk Analysis", IEEE 2013.
[25] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, "Improvisation of Security aspect in Steganography applying DES", IEEE 2013.
[26] Praloy Shankar De, Prasenjit Maiti," DEDD Symmetric-Key Cryptosystem", International Journal of Advanced Computer Research (IJACR) ,Volume-3 Number-1 Issue-8 March-2013.
[27] Seetaiah Kilaru, Yojana Kanukuntla, K B S Chary," An effective algorithm for Image security based on Compression and Decomposition method", International Journal of Advanced Computer Research (ISSN (IJACR) Volume-3 Number-1 Issue-8 March-2013.
[28] Singhal, Mukesh and Shivaratri, Niranjan G., Advanced Concepts in Operating Systems, McGraw-Hill, p. 405.
[29] Rivest, R.L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol 21, No. 2, February 1978, p. 120-26.
[30] Dubey, A.K.; Dubey, A.K.; Namdev, M.; Shrivastava, S.S., "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment," Software Engineering (CONSEG), 2012 CSI Sixth International Conference on , vol., no., pp.1,8, 5-7 Sept. 2012.