A survey on Symmetric Key Algorithms for Image Encryption

Aarti Devi, Ankush Sharma, Anamika Rangra

***Abstract*— Cryptography is an emerging technology which is important for network security. Some well-known cryptographic algorithms have been analyzed in this paper to demonstrate the basic differences between the existing encryption techniques. In this paper we discuss and survey symmetric key algorithms (DES, AES and Blowfish) for Image Encryption and Decryption. In today's world it is a crucial concern that while transfer image from one network to another network over the internet, the proper encryption and 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.**

***Index Terms*— DES, Blowfish, AES, Performance factor.**

I. INTRODUCTION

Cryptography & Network Security is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The conventional methods of encryption can only maintain the data security [1]. Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control and so forth.[2] The terms used in cryptography are plain image, cipher (encrypted image), encryption, decryption and Alice, Bob, and Eve. A process of converting Plain image into Cipher (encrypted image) is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. Encryption takes place at the sender side. A reverse process of encryption is called as Decryption. It is a process of converting Cipher (encrypted image) into Original image. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message. [3]

II. SYMMETRIC KEY ALGORITHMS

1) ***DES (Data Encryption Standard)*:-** DES was the first encryption standard published by NIST (National Institute of Standards and Technology) [4].It is a symmetric algorithm; It uses one 64-bit key. Out of 64 bits, 56 bits make up the independent key, which determine the exact cryptography transformation; 8 bits are used for error detection. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The output is a 64-bit block of cipher text.

2) ***AES (Advanced Encryption Standard):-*** It was recognized that DES was not secure because of advancement in computer processing power [6]. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies [20]. It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible.

3) ***Blowfish Algorithms:*** - Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less.

III. COMPARISON BETWEEN SYMMETRIC KEY

Performance analysis and comparison between symmetric key algorithms such as DES, AES and Blowfish are as follow

Factor	**DES**	**AES**	**Blowfish**
Encryption	Slow	Fast	Fast
Decryption	Slow	Fast	Fast
Key Size	56 bits	128, 192, 256 bits	32-448 bits
Round	16	10,12,14	16
Speed depends on Key	Yes	Yes	No
Security	Insecure	Secure	Believed secured, but less Attempted cryptanalysis than other algorithms.
Hardware and software	Designed for hardware and	Fast in both in	Designed for software.

implementation	quite slow in software	hardware and software.	
Exiting Attacks	Brute force attack, differential crypanalysis, linear crypt-analysis	Side channel attacks	Second-order differential attack

IV. LITERATURE SURVEY

Rathod et al. [6] mainly focus on security management. He used the HIEA(Hyper Image encryption Algorithm), which is combination of image permutation. Also, introduce a new permutation technique based on the combination of image permutation and a new developed encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". From the selected image we will binary value blocks, which will be rearrange into a permuted image using a permutation process, and then the generated image will be encrypted using the "Hyper Image Encryption Algorithm (HIEA)" algorithm.

Acharya et al 2009 [7] proposed a novel advanced Hill (AdvHill) encryption technique which uses an involuntary key matrix. The scheme is a fast encryption scheme which overcomes problems of encrypting the images with homogeneous background. A comparative study of the proposed encryption scheme and the existing scheme is made. The output encrypted images reveal that the proposed technique is quite reliable and robust.

Subasree et al. 2010 [8] uses a three cryptographic primitives such as integrity, confidentiality and authentication. These three primitives can be achieved with the help of Elliptic Curve Cryptography, Dual-RSA algorithm and Message Digest MD5. That is it uses Elliptic Curve Cryptography for encryption, Dual-RSA algorithm for authentication and MD-5 for integrity. This new security protocol has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.

Afaf et al. 2011 [9] introduces a new method to enhance the performance of the Blowfish Algorithm. This is done by building a new structure for the 16 rounds in the original algorithm by replacing the OR operation with a new introduced operation. This structure makes use of multiple secrete keys. The principle of Cellular Automata (CA) is used to generate these multiple keys in a simple and effective way. The proposed method provides high quality encryption, and the system is very resistant to attempts of breaking the cryptography key.

Anand et al. 2012 [10] mainly focuses on two commonly used symmetric encryption algorithms such as Blowfish and Rejindael. These algorithms are compared and performance is evaluated. Experimental results are given to demonstrate the performance of these algorithms.

Qaid et al. 2012 [11] aims at improving the level of security and secrecy provided by the digital color signal-based image encryption. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image based data as well as in storage. This new proposed encryption algorithm can ensure the lossless of transmissions of images. The proposed encryption algorithm in this study has been tested on some images and showed good results.

Sahu et al. 2012 [12] presents image encryption/decryption scheme using biometric template (Palm Print). The proposed scheme is especially useful for encryption of large amounts of data, such as digital images using proposed key generation algorithm. This scheme satisfies the characters of convenient realization, less computation complexity and good security. The salient features of the proposed image encryption method are loss-less, asymmetric public key encryption, a very large number of secret keys, and key-dependent pixel value replacement.

Lalit et al. 2013 [13] provides a fair comparison between five most common and used symmetric and asymmetric key algorithms: Two fish & Blowfish, IB_mRSA, RSA, RC. A comparison has been made on the basis of these parameters: rounds block size, key size, and encryption/decryption time, CPU process time in the form of throughput. These results show that IB_mRSA is more suitable than other algorithms. Simulation program is implemented using C#.NET programming.

Mahajan et al. 2013 [14] implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each algorithm.

Chandel et al. 2013 [5] discusses 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.

Pakshwar et al. 2013 [15] survey of Different Image Encryption and encryption techniques that are existing is given. It additionally focuses on the functionality of Image encryption and decryption techniques.

Saraf et al. 2014 [16] implements the text and image encryption and decryption using AES. If the images have large data size and also has real time constrain problem hence similar method cannot be used to protect images as well as text from unauthorized access. However with few variations in method AES can be used to protect image as well as text.

V. PROBLEM DOMAIN

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

1) There is research work done on DES, AES and Blowfish algorithm for text simulation. [20]

2) Several research works had been done in the image encryption and decryption earlier, but with the help of DES, AES and Blowfish algorithm for image encryption and decryption we can reduce the encryption and decryption time by using latest tool i.e. NetBeans IDE 7.4.

3) The algorithms must support color image data with logical key.

4) It can be applied on Network Communication for sending encrypted images. So it can be useful in the military services.[21]

VI. PERFORMANCE FACTOR

Various important factors on which performance of cryptographic algorithms depend are:

1) ***Tunability:*** It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications.

2) ***Computational Speed:*** In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.

3) ***Key Length Value:*** In the encryption methodologies the key management is the important aspect that shows how the data is encrypted. The image loss the encryption ratio is based on this key length. The symmetric algorithm uses a variable key length which is of the longer. Hence, the key management is a considerable aspect in encryption processing.

4) ***Encryption Ratio:*** The encryption ratio is the measure of the amount of data that is to be encrypted. Encryption ratio should be minimized to reduce the complexity on computation [22].

5) ***Security Issues:*** Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In our analysis we measure cryptographic security in three levels: low, medium and high [23].

VII. CONCLUSION

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. 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.

In this paper we survey various symmetric key algorithms such as DES, AES and Blowfish algorithms to enhance the performance and encryption and decryption time of the image. Based on the above study we provide the following future directions which can be helpful in better detection:

1) *Experiments on audio*
2) *Experiments on video*
3) *Improve the encryption and decryption time.*

REFERENCES

[1] Sumedha Kaushik & Ankur Singhal "Network Security Using Cryptographic Techniques," *International Journal of Advanced Research and Computer Science and Software Engineering (IJARCSSE),* Volume 2, Issue 12, December 2012.

[2] Suman Chandrasekhar, Akash H.P, Adarsh.K, Mrs. Smitha Sasi "A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem," *IOSR Journal of Computer Engineering (IOSR-JCE),* Volume 11, Issue 2 (May. - Jun. 2013).

[3] Kritika Acharya, Manisha Sajwan & Sanjay Bhargava "Analysis of Cryptographic Algorithms for Network Security," *International Journal of Computer Applications Technology and Research (IJCATR),* Volume 3– Issue 2, 130 - 135, 2014.

[4] Shanta, yoti Vashishtha,"Evaluating the performance of Symmetric Key Algorithms:AES (Advanced Encryption Standard) and DES (Data Encryption Standard)" *IJCEM International Journal of Computational Engineering & Management,* Vol. 15 Issue 4, July 2012 ,pp.43-49

[5] A. Nadeem, "A performance comparison of data encryption algorithms, "*IEEE information and Communication Technologies* , pp. 84-89, 2006.

[6] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", *International Journal of Computer Technology and Electronics Engineering (IJCTEE),* Volume 1, Issue 3.

[7] Acharya Bibhudendra, Panigrahy Saroj Kumar, Patra Sarat Kumar, and Panda Ganapati "Image Encryption Using Advanced Hill Cipher Algorithm" *International Journal of Recent Trends in Engineering (IJRTE),* Vol. 1, No. 1, May 2009.

[8] Subasree S. and Sakthivel N. K. "Design of a New Security protocol using Hybrid Cryptography Algorithms" *IJRRAS 2 (2)* ● February 2010.

[9] Afaf M. Ali Al-Neaimi, Rehab F. Hassan, "New Approach for Modifying Blowfish Algorithm by Using Multiple Keys", *International Journal of Computer Science and Network Security (IJCSNS),* VOL.11 No.3, March 2011.

[10] M. Anand Kumar, Dr.S.Karthikeyan "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms", *I. J. Computer Network and Information Security (IJCNIS),* 2012, 2, 22-28.

[11] Gamil R.S. Qaid , Sanjay N. Talbar "Encryption and Decryption of Digital Image Using Color Signal" *International Journal of Computer Science Issues(IJCSI),* Vol. 9, Issue 2, No 2, March 2012.

[12] Amrita Sahu, Yogesh Bahendwar, Swati Verma, Prateek Verma " Proposed method of Cryptography Key Generation for Securing Digital Image", *International Journal of Advanced Research and Computer Science and Software Engineering (IJARCSSE),* Volume 2, Issue 10, October 2012,.

[13] Lalit Singh Dr. R.K. Bharti, "Comparative performance analysis of Cryptographic Algorithms", *International Journal of Advanced Research and Computer Science and Software Engineering (IJARCSSE),* Volume 3, issue 11, November 2013.

[14] Dr. Prerna Mahajan & Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security", *Global Journal of Computer Science and Technology Network, Web & Security (GJCSTNWS),* Volume 13 Issue 15 Version 1.0 Year 2013.

[15] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya "A Survey On Different Image Encryption and Decryption Techniques", *International Journal of Computer Science and Information Technologies (IJCSIT*), Vol. 4 (1) , 2013, 113 – 116.

[16] Kundan kumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra "Text and Image Encryption Decryption Using Advanced Encryption Standard*", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* Volume 3, Issue 3, May – June 2014.

[17] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *IEEE Trans. on Neural Networks*, vol. 4, pp. 570-578, July 1993.

[18] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34-39, Jan. 1959.

[19] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.

[20] Jawahar Thakur , Nagesh Kumar," DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, Volume 1, Issue 2, December 2011.

[21] Gajendra Singh Chandel , Pragna Patel "A Review: Image Encryption with RSA and RGB randomized Histograms", *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, Vol. 2, Issue 11, November 2013.

[22] AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram, "Comparative Analysis of Performance Efficiency And Security Measures of Some Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA), VOL.2, Issue 3,May-Jun 2012, Page 3033-3037.

[23] G. Ramesh, R. Umarani, "Performance Analysis of Most Common Encryption Algorithms on Different Web Browsers "I.J. Information Technology and Computer Science, Issue Nov 2012, Page 60-66.

Aarti Devi received the B.Tech degree in Computer Science Engineering from IEET, Baddi (H.P.) in 2011. After that she worked as lecturer in Gautam Girls College Hamirpur (H.P.) for six months. She is now as a research scholar in Carrer Point University Hamirpur (H.P.).

Ankush Sharma received the B.Tech degree in Computer Science Engineering from GHEC, Solan (H.P.) in 2010. After that he worked as lecturer in MIT, Bani, Hamirpur (H.P.) for one year. He is now as a research scholar in Carrer Point University Hamirpur (H.P.).

Anamika Rangra received the B.Tech and M.tech degree in Information & Technology from JAYPEE University, Waknaghat, Solan (H.P) in 2012 and 2014. She had been two research paper published in security in Cloud Computing. She has an IEEE Membership. She is now as a Assistant Professor in Carrer Point University Hamirpur (H.P.).

