A Survey on image cryptography using Encryption & Decryption techniques

Manish Goyal [1], Umesh Kr. Gera [2],
M.Tech[1], Assit.prof.[2] Department of Computer Science & Engineering, Faculty of Engineering & Technology,
Rama University,Kanpur (U.P.) India

***Abstract*- This paper is mainly focus on the different cryptographic algorithm used for image encryption & desktop in the field of image security. Security as an information technology has acquired an important place as the digital image has become a medium that has come with communication, researchers and various technologies. Protecting the image & a lot of data on the internet from time to time cryptography refers to the study of many aspects related to mathematical techniques. & keeping data confidential & keeping information security like, data authentication this paper presents a survey of different images in addition it provides different aspects used for image security.**

Keywords: Cryptography, encryption, descryption.

I. INTRODUCTION

Cryptography is the technique of securing information & communication through the use of code so that only the person for whom the information is intended can understand the process it. In this way unauthorised access to information can be prevented. The techniques used to protect information in cryptography are derived from mathematical concepts & a set of rules-based calculations known as algorithms. The algorithms are used for cryptographic key generation, digital signatures, verification to protect data privacy, web browsing on the internet & for protecting confidential transactions such as credit card & debit card transactions. That's why cryptography has an important role of image, audio, video & test.

In general there are three types of cryptography:

1. Symmetric key
2. Hash functions
3. Asymmetric key

II. SYMMETRIC KEY

This is also termed as private or secret key cryptography. Here both the information receiver & the sender make use of a single key to encrypt & decrypt the message. The frequent kind of cryptography used in this method is AES (advanced encryption system).The approaches implemented through this type are streamlined & quicker too. Some types of symmetric key are such as. Block, DES (Data Encryption System), RC2, IDEA, Block cipher.

III. ASYMMETRIC KEY

This is also termed as public key cryptography. It follows a varied & protected method in the transmission of information. Using a couple of keys, both the sender & receiver go with encryption & descryption processes. A private key is stored with each person & the public key is shared across the network so that a message can be transmitted through public keys. The frequent kind of cryptography used in this method is RSA. The public key method is more secure than that of a private key. Some of the asymmetric key cryptography is such as. DSA, RSA. PKCs.

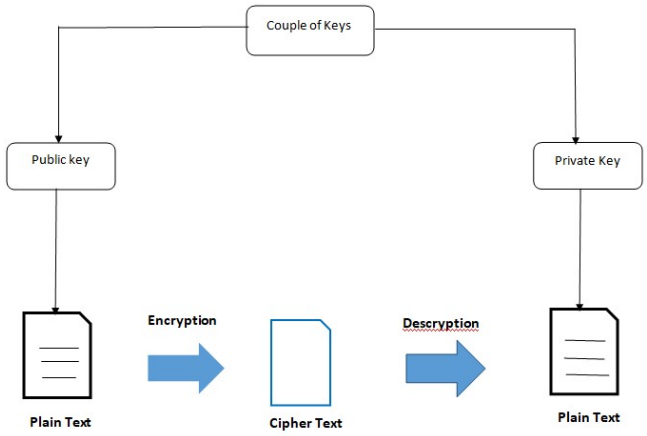

Figure 1: Symmetric & Asymmetric encryption

IV. AUTHENTICATION USING KEY

The encrypted information has to be decrypted through keys; the normal information is easily understood by everyone whereas the encrypted information is known only by the destined user. This tool has two kinds of encryption techniques.

- Symmetric key cryptography
- Asymmetric key cryptography

2. The cryptography algorithms include the following.-

2.1 Triple DES: Taking over the conventional DES mechanism, triple DES was currently implemented in the security approaches. These algorithms permit hackers to ultimately gain the knowledge to overcome in easy approaches. This was extensively implemented approach by many of the enterprises. Triple DES operates with 3 key

having 56 bits per each key. The entire key length is a maximum of bits, whereas experts would contend that 112-bits in key intensity are more probable. This algorithm control to make a reliable hardware encryption answer for banking facilities & also other industries.

2.2 RSA: One of the public key encryption algorithms used to encrypt information transmitted through the internet. It was a widely used algorithm in GPG & PGP methodologies. RSA is classified under symmetric type of algorithms as it performs its operation using a couple of keys. One of the keys is used for encryption & the other for description purposes.

2.3 Blowfish: To replace the approaches of triple DES, Blowfish was mainly developed. This encryption algorithm split up messages into clocks having 64 bits & encrypts this clock separately. The captivating feature that lies in Blowfish is its speed for everyone, many gained the benefits of implementing this, and every scope of the IT domain raging from software to e- commerce is making use of this algorithm as it shows extensive features for password protection. All these allow this algorithm to be most prominent in the market.

2.4Twofish: This algorithm implements keys to provide security & as it comes under the symmetric method, only one of key is necessary. The keys of this algorithm are with the maximum length of 256 bits. Of the most available algorithm, two fish is mainly known by its speed & perfect to be implemented both in the hardware & software application. Also, it is an openly accessible algorithm & has been in execution by many.

2.5 AES (Advanced Encryption Standard): This is the most trusted algorithm technique by U.S administration & many other enterprises even though this works efficiently in 128-bit encryption from, 192 & 256 bits are mainly used for huge encryption activities. Being so invulnerable to all Hacking systems, the AES technique receives extensive applause for encrypting information in the private domain.

V. LITERATURE SURVEY

3.1 A survey on image encryption technique

In this paper author described somewhere about some traditional techniques like DES, AES or idea to provide high security etc. may be in the form of text or images. These techniques are difficult to us them directly in multimedia data. It is necessary because of some drawbacks in place, anchor speed & other aspect is on the other. Conversion is mainly used of image encryption which is very simple & easy to implement but due to the success of these techniques the description processes is also simple so one third person can easily crack the algorithm. High security is combined with this technology. Other techniques we learned in this paper that both compression & encryption are combined &formed a new technology which is effective but needs additional operations. Requirements according to every technology, it has some advantages & some disadvantages as well, its working method is different.

3.2 A Lightweight encryption algorithm for secure IOT:

In this paper the need for lightweight secure cryptography is discussed extensively in the context of an image. The drawbacks of the IOT are also highlighted in constrained devices. Secure system maintain the confidentially of data & ensure that the exchange of data during the processing of the message retains its originality RFID is composed of many Small devices that remain unattended for extended periods of time, making it easier for adversaries to access data stored in memory. The proposed algorithm provides a simple structure that is suitable to be implemented in IOT environments. Some well-known block ciphers, including AES, 3-way grasshopper use current, safe, shard & square substitution permutation (SP) network. The alternating round of multiple substitutions & transfers satisfies Shannon's illusion & diffusion. Properties that ensure that the cipher text is change d in pseudo-random way.

3.3 Review on image encryption & description technique using AES algorithm:

This paper is mainly based on encryption & description of image using advanced encryption. Standard algorithm advanced encryption standard the AES algorithm is a symmetric block cipher that modifies the image to have a block size of 128 bits using three different cipher key size of length 128, 192 or 256 bits. Depending on the length of the key shape used, the number of execution rounds of the algorithm are 10, 12, or 14 respectively, the proposed systems system has a block size of 128 bits & a block size of 256 bits the key are of size. The algorithm is applied for both the image encryption & description. Since the size of the key is 256. Belongs to bits it will take 14 rounds. Internet access & wireless communication is growing rapidly. Cryptography is a technique used exclusively secure communication, in this paper its done surveyed about existing work on encryption technologies like AES, 3DES, Blowfish & the key size is very small compared to other techniques.

VI. CONCLUSION

We worked on major techniques of data security that is cryptography, encryption & descryption in our system these techniques provides high security for our data. The information is initially encrypted by using secure internet of things algorithms which is secure IOT algorithm & LSB gives a way to secure information from illegal users & provide better PSNR value. It is very difficult to recover the hidden image. Image & data plays an important role in life & they are used in many applications in our daily life. Therefore it is necessary to verify its integrity to verify its integrity & confidentiality. This paper contains some

important image cryptography survey. Provided in the past decades. These encryption methods are thoroughly studies & analysed to boost performance. & is unique in the way of it makes it suitable for many applications. Every day new technology is developing so fast & secure traditional encryption technology works with high security data rate. This survey Provide a way to realize the various aspects used from the chaotic to the genetic algorithmic approaches & DNA sequences for image encryption.

VII. ACKNOWLEDGEMENTS

Authors are thankful to the head of department of Rama University Kanpur, India for his kind support & useful technical discussion during the course of this work; thanks are also due to friends & colleagues of our department for their cooperation, fruitful technical discussion & guidance.

REFERENCES

[1] Abboud, G.; Marean, J.; Yampolskiy, R.V.;"Steganography and Visual Cryptography in Computer Forensics," Systematic Approaches to Digital

[2] Forensic Engineering (SADFE), 2010 Binary Images," Innovative Computing, Information and Control,2006.ICICIC

[3] Yogita Verma1, Neerja Dharmale2, 1M Tech Scholar Digital Electronics RCET Bhilai, India 2Assistant Professor (ET&T) RCET Bhilai, India, A Survey Paper Based On Image Encryption and Decryption Using Modified Advanced Encryption Standard, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013)

[4] Muhammad Usman_, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan_ and Usman Ali Shahy, Faculty of Engineering Science and Technology, SIT: A Lightweight Encryption Algorithm for Secure Internet of Things, (IJACSA)

[5] International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.

[6] Sneha Ghoradkar, Aparna Shinde, Review on Image Encryption and Decryption using AES Algorithm, International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT2015).

[7] SandeepBhowmik and Sriyankar Acharya, “Image Cryptography: The Genetic Algorithm Approach”, IEEE, 2011, 978-1-4244-8728-8.

[8] Ibrahim S I Abuhaiba, Maaly A S Hassan, “Image Encryption Using Differential Evolution Approach In Frequency Domain”, Signal & Image Processing An International Journal (SIPIJ) Vol.2, No.1, March 2011.