Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 13, December 2019

A STATE-OF-THE-ART REVIEW ON IMAGE ENCRYPTION TECHNIQUES AND BIO CRYPTOGRAPHY

Dr. Raghu N
Assistant Professor, Department of EEE,Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email id: raghu1987n@gmail.com.

Abstract

Cryptography defends against unauthorized access to data stored on the network. High-security data transfer is very important. Biometrics is a distinctive feature of human beings and is a well-recognized individual authenticator. The sharing of all medical data has been carried out widely in the world. The Advanced Encryption Standard (AES) encryption algorithm is used as the most efficient cryptographic algorithm for high security. Thanks to its long-term security, this algorithm is widely preferred and has a broad range of applications and protocols. Due to the massive sharing of confidential information, the security of data over the network has become a significant problem. In different fields, such as hospitals, science, medical applications, etc., cryptography is used for secret transmission of knowledge. This paper is an analysis of familiar encryption strategies from which researchers will learn the principle of effective methods to be used..

Keywords: *Crptography, Data safety, DNA, Encryption, Image, Media, Compression.*

I. INTRODUCTION

In today's new digital world, the exchange of knowledge is growing. The security of information is therefore one of the challenging aspects. Cryptography is an effective tool that is used in a safe format to store and transfer information so that only the intended user can access and process the data. The data is encrypted in cryptography with many secure algorithms that either cost heavily on the power consumption side or appear to be highly complex, making the performance or throughput low. For low power consumption, high security and improved throughput on encrypted files, the pipelining architecture is implemented into the device. In mobile and wireless based systems, this form of design plays a crucial role as power consumption is the key constraint to be minimized [1].

Figure 1: Illustrates the real and encrypted images [2]

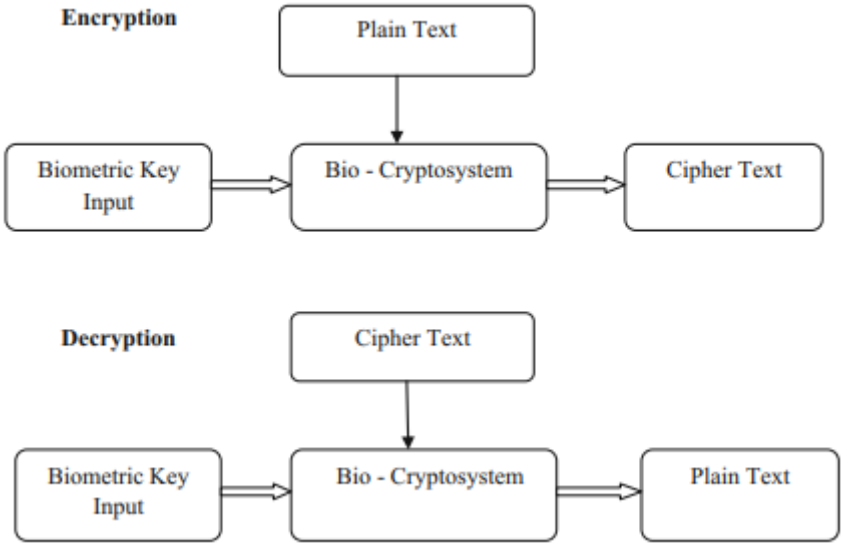

Figure 2: Illustrates the Block diagram of bio cryptosystem [3]

$$MSE = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[P(i,j) - E(i,j)]^2}{W \times H}$$

$$MAE = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W}|p(i,j) - E(i,j)|$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

$$cov\,(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\,(y_i - E(y))$$

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)} \neq 0, \sqrt{D(y)} \neq 0$$

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\,\%$$

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255} \right] \times \frac{100\%}{M \times N}$$

$$D(y) = \frac{1}{K} \sum_{i=1}^{K} (y_i - E(y))^2$$

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [4].

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y)$, $D(x)$ and $D(y)$ can be evaluated by using the following equations [5].

$$C(x,y) = \frac{\sum_{i=1}^{K} (x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K} \sum_{i=1}^{K} (x_i - E(x))^2$$

II. LITERATURE REVIEW

Zhou et al. investigated another novel image encryption algorithm based on chaos and Line map. Data security boundaries have become increasingly blurred in the era of big data. Our defense of privacy is undergoing a new round of testing. In particular, multimedia big data photos also hold several secrets or data regarding privacy. In the processing and transmission of image content, how to ensure protection and authorize access to sensitive data becomes a hot issue of urgency. In this post, we propose a new algorithm for symmetrical image encryption based on the skew tent map. The proposed algorithm is ideal for encryption of any image size using a new chaos-based line map [6].

III. DISCUSSION AND CONCLUSION

In the world of modern electronics, security is very necessary. By integrating multiple hardware optimization design strategies to achieve ultra-low power, high throughput and energy efficient design with multiple levels of security, the AES algorithm is further enhanced. In this review, an overview is given of the perceptual methods of data hiding techniques specifically discussed in cryptography. Also revealed are familiar encryption methods, powerful bio-cryptography algorithms and image encryption schemes. Using various biometric traits such as face, voice etc., and this technique can also be implemented. The paper also presents a succinct definition of using effective techniques for hardware design and can be used for further research purposes

IV. REFERENCES

[1] C. C. Chang, M. S. Hwang, and T. S. Chen, "A new encryption algorithm for image cryptosystems," J. Syst. Softw., 2001, doi: 10.1016/S0164-1212(01)00029-2.

[2] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "A hash-based image encryption algorithm," Opt. Commun., 2010, doi: 10.1016/j.optcom.2009.10.106.

[3] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," Appl. Soft Comput. J., 2012, doi: 10.1016/j.asoc.2012.01.016.

[4] S. Kumar, A. Gupta, and A. Arya, Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-9801, 2016.

[5] E. N. Kumar and E. S. Kumar, "A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach," 2013.

[6] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," Neurocomputing, 2015, doi: 10.1016/j.neucom.2014.11.095