BIOMETRIC AUTHENTICATION FOR IMAGE SECRECY IN CLOUD FRAMEWORK: A REVIEW PAPER

Arun N
Faculty of Engineering and Technology, Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: n.arun@jainuniversity.ac.in

Abstract

Cloud computing is a major blooming technology that has multiple applications and is understandably so hyped in today's industry. Photos, especially due to widespread social media, are a big part of today's internet data traffic, and so their protection is crucial. The photos in the cloud are, however, a big security problem in the current scenario. Since the user who uploaded the image does not have control over image protection, the cloud provider must maintain full security in terms of authentication and attack prevention. The main aim of this paper is to provide a method to improve the protection of cloud images. This paper presents an idea of using biometric authentication to secure images on a cloud platform. Different steps are explained in biometric authentication and secure image upload and access, and all steps are finally integrated as a case study that sheds light on the entire process in which methods are best-regarding results and compatibility. In this paper, the proposed algorithm presents the concept of image authentication in two basic steps of image compression using the standard discrete wavelet transformation method, followed by image encryption using the SHA and blowfish hybrid method. This image is then stored in the cloud database and accessed any time it is requested by the user. This paper offers a formal and detailed view of encryption techniques, forms of biometrics and protected data as well as images.

Keywords: *Image, Encryption, Authentication, Protection, Biometric, Algorithms, Security*

I. INTRODUCTION

The drastic change in the eminence of the technological world is primarily as a result of the advancement in the speed and the performance of the internet [1]. The real-time fast processing and storage of multimedia data on the internet in recent times have heavily relied on cloud computing. Even though the cloud is barely a decade old, it has influenced the computing world such as no other technology [2].

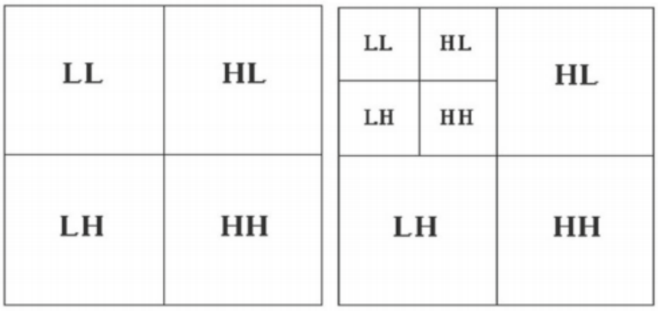

Figure 1: Illustrates the single level and two level decomposition

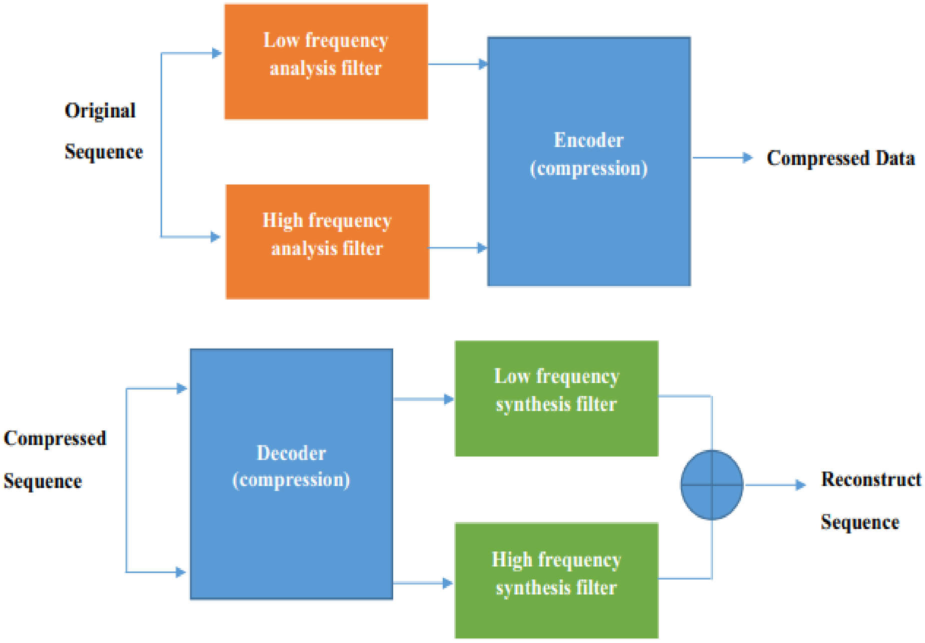
Original Sequence
Low frequency analysis filter
High frequency analysis filter
Encoder (compression)
Compressed Data
Compressed Sequence
Decoder (compression)
Low frequency synthesis filter
High frequency synthesis filter
Reconstruct Sequence

Figure 2: Illustrates the DWT procedure on image for compression as well as decompression [3]

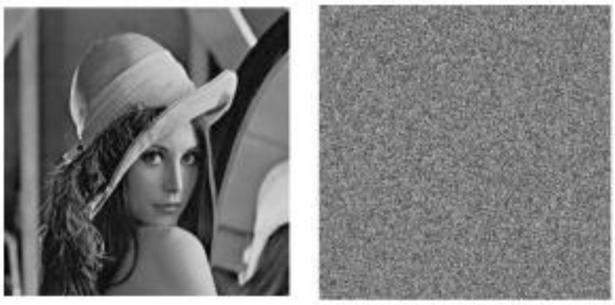

Figure 3: Illustrates the real and encrypted images

Figure 1: Illustrates the single level and two level decomposition. Figure 2: Illustrates the DWT procedure on image for compression as well as decompression. Figure 3: Illustrates the real and encrypted images.

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

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

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

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

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

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

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

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

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

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

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].

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

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

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

II. LITERATURE REVIEW

Sayed et al. investigated a novel chaotic image encryption approach based on many discrete complex maps. One of the most significant aspects of the technologically advanced era is the transmission of information over an unreliable means of communication. In the form of binary bits, electronic knowledge moves. One of the most significant issues in today's world is the security of such digital content. We have used many messy iterative maps in this article to suggest a novel technique of image encryption. Confusion and diffusion, which is one of the most basic aspects of the encryption process, have been applied to the proposed encryption in the framework provided. Our expected method has been checked against distinct performance analysis and contrasted with current results. The developed framework is capable of providing digital images with excellent privacy [6].

III. DISCUSSION AND CONCLUSION

Several studies and research papers have studied the notion of cloud image protection based on anonymity, honesty, and availability. A method of biometrics authentication coupled with image encryption is proposed in this paper to ensure that image protection on the cloud architecture is proposed. Many types of attacks on a daily basis conclude that, relative to other forms of data, private images need special attention than cloud data. As an authentication method, biometrics have been on the rise to authorize the user and set up some authorization checks to not allow any other individual to authorize it. If the authorization process itself is made solid and faultless, then the overall system's level of protection improves. Successive interventions such as image compression and encryption achieve an additional degree of efficiency. In fact, when iris detection is taken into account, most modern systems have a biometric scanner installed within them. In this article, as most smartphones and laptops already have an iris scanner inside them, we have chosen iris as the biometric used for authentication, and the chances of the iris of two people being the same are also very thin. The computer will scan the user's iris after the image is queued for upload or access by the user, compare it to its database image and then allow the user to upload or access the image. In terms of security as well as image format compatibility, the type of hybrid algorithm proposed has proven to be highly efficient..

IV. REFERENCES

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

[2] A. Jain, M. Ahmad, and V. Khare, “A ridgelet based symmetric multiple image encryption in wavelet domain using chaotic key image,” 2012, doi: 10.1007/978-3-642-

32112-2_17.

[3] 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.

[4] M. Khan and T. Shah, "A Literature Review on Image Encryption Techniques," Autoimmunity Highlights. 2014, doi: 10.1007/s13319-014-0029-0.

[5] Y. P. Zhang, Z. J. Zhai, W. Liu, X. Nie, S. P. Cao, and W. Di Dai, "Digital image encryption algorithm based on chaos and improved DES," 2009, doi: 10.1109/ICSMC.2009.5346839.

[6] W. S. Sayed, H. A. H. Fahmy, A. A. Rezk, and A. G. Radwan, "Generalized smooth transition map between tent and logistic maps," Int. J. Bifurc. Chaos, 2017, doi: 10.1142/S021812741730004X