Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 9, September 2019

IMAGE ENCRYPTION METHOD BY USING BIT-PLANE COMPRESSION: A REVIEW ARTICLE

Harish Naik
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: harish.naik@jainuniversity.ac.in

Abstract

Remembering or privately saving the key for encrypting the hidden picture is quite a task. Moreover, the encrypted image could arouse the suspicion of the invaders. In this paper, using the bit-plane compression and Lagrange interpolation formula, a novel hidden image sharing scheme with additional steganography and repairable capabilities is proposed. The proposal suggests that the user choose an ostensible image, such as a popular character image, to disguise his hidden image as the cover image to improve protection. Specifically, to create meaningful shadow images, a protected image is split into three shares and concealed in the cover image. Then, three shadow images, such as the mobile, the laptop, and cloud storage, are distributed to three separate devices. The user can recover the initial hidden image and the cover image losslessly by collecting any two shadow images. Furthermore, when the smartphone or laptop is lost, the proposed device is easily repairable. The review of the framework reveals that not only does the proposal achieve theoretical information security, it is also technically realistic.

Keywords: *Bit-Plane, Encryption, Hidden-Image, Image, Protection, Interpolation, Steganography.*

I. INTRODUCTION

It has become easy and convenient for us to take an image and post it through the social media network with the popularization of smartphones, which accelerates the distribution of information and promotes everyday life [1]. Nevertheless, things do not go that way often. In fact, some images

need to be secured, otherwise their leakage could expose the private information of the user, and even impact the security of the information [2].

Fig 1: Illustrates the Original Images and Encrypted Image [3]

IMAGE ENCRYPTION METHOD

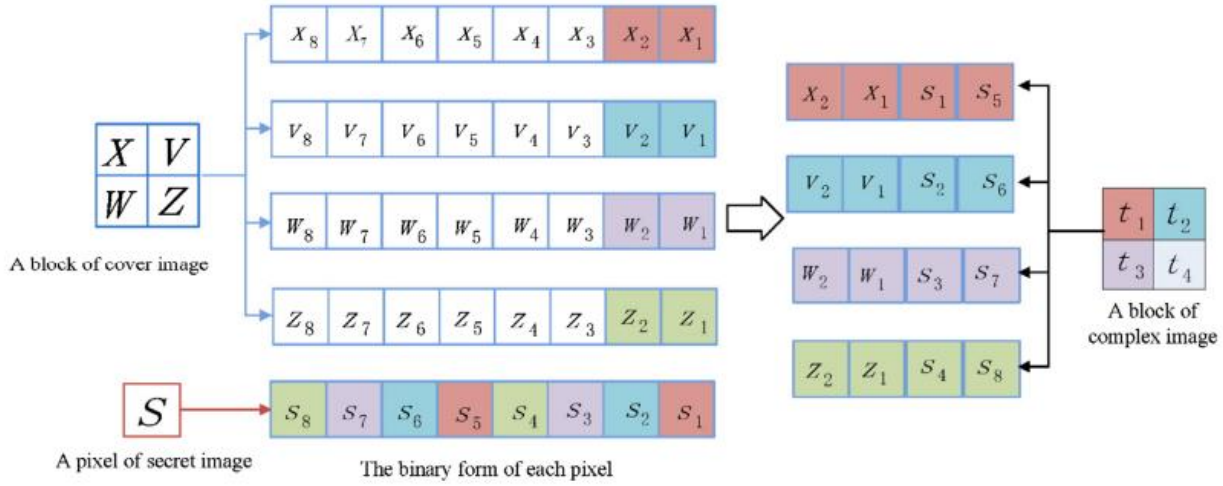

Fig 2: Illustrates the procedure of the generation of complex image [4]

The compression of the bit-plan refers to compressing both the hidden image and the cover image at the bit level into a complex image. This work is important to ensure that the hidden image and cover image, as well as the system's repair capacity, can be restored losslessly. The justifications are as follows.

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

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

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

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

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

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

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

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

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [5].

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

Where $C(x,y), D(x)$ and $D(y)$ can be evaluated by using the following equations [6].

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

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

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

II. LITERATURE REVIEW

Chen et al suggested a symmetric image encryption scheme based on 3D chaotic cat maps. Due to some intrinsic features of images, such as bulk data capacity and high redundancy, which are usually difficult to manage by conventional methods, image encryption varies from that of texts. Due to the extremely desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly protected image encryption. In this paper, for designing a real-time protected symmetric encryption scheme, the two-dimensional chaotic cat map is generalized to 3D [4].

III. DISCUSSION AND CONCLUSION

A novel hidden image safety threshold scheme based on Bit-plane compression and Lagrange interpolation is proposed in this paper, which is effective, accurate, and practical. The secret image is split into three meaningful shadow images and stored in three distinct devices instead of encrypting the secret image, or saving it in a safe location and out of plain sight with the risk of being lost or forgotten. The user can recreate the hidden image losslessly by merging two shadow images without using any decryption keys. However, even if one shadow image is lost, no one can learn the original image's content, but by combining the other two shadow images, the user can access it. In addition, our proposal allows the user to restore the cover image losslessly, and it can be expanded into a (t, n)-threshold hidden image security system. More significantly, when the smartphone or laptop of a user is lost, it is easily repairable. The experimental results and device review indicate that the plan works well and guarantees its viability.

IV. REFERENCES

[1] 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.

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

[3] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, 2014, doi: 10.1016/j.optlaseng.2013.12.003.

[4] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, 2004, doi: 10.1016/j.chaos.2003.12.022.

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

[6] 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.