INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 893-898
RECEIVED : 27/03/2016. PUBLISHED : 05/04/2016
April 5, 2016

ENCRYPTION AND RETRIEVAL OF IMAGES IN CHAOTIC MAP BASED IMAGE SECURITY WITH TAMPER DETECTION

[1]Pradeep.K, [2]Narasimhan.C
Dept of Applied Electronics, Bharathidasan Engg College, Tirupattur,
Associate Prof, Dept of Applied Electronics, Bharathidasan Engg College, Tirupattur.

Abstract:

In this project, an image encyption technique based upon chaotic map transform is proposed and analyzes that, how it is resistant to attacks along with back ground subtraction. The reversible decryption provides an over complete representation of the image which facilitates the identification of significant image features via a simple correlation operation across scales. Although the encryption algorithm is image adaptive, it is not necessary for the original image to be available for successful detection of the received image. But our project needs the received image and the original image in order to calculate the PSNR. The performance and robustness of the proposed technique is tested by applying common image-processing operations such as filtering, re-quantization, and JPEG compression. A quantitative measure is proposed to objectify performance; under this measure.

Key words – Encryption, Robustness, Re-quantization.

1. INTRODUCTON

Digital image authentication is increasingly becoming more important with the tremendous development of the Internet. The ability of fragile encryption to detect changes in the encryptioned image to provide authenticity and integrity of the image makes it go a long way toward solving the image authentication problem.In contrast to a semifragile encryption, which only seeks to detect a predefined set of illegitimate distortions to the host image, a fragile encryption is designed to detect any change to the host image. Hence, a variety of fragile encryption methods has been proposed by embedding identifying information in the least-significant bits (LSBs) of the image. Unfortunately, these methods are somewhat unsecured as the use of LSBs could be easily detected and manipulated. In a fragile encryption scheme using a statistical model was proposed. However, the scheme was only able to localize distorted pixels altered in the five most significant bits. In recent years, as digital media are gaining wider popularity, their security related issues are becoming greater concern. Digital encryption is a technique which allows an individual to add copyright notices or other verification messages to digital media. Image authentication is one of the applications of digital encryption, which is used for authenticating the digital images. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. The way to realize this feature is to embed a layer of the authentication signature into the digital image using a digital encryption. In the case of the image being tampered, it can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values. There are many spatial and frequency domain techniques available for authentication encryption.iIn message authentication, only the image integrity is verified, but sometimes this is not sufficient in digital images and tamper localization is also required. The situations

include forensics, crime, and insurance. Tamper localization is used to identify the specific positions where the tamper has occurred. To achieve tamper localization many existing schemes use block-based approach. One of the first fragile encryption techniques proposed for detection of image tampering was based on computing check-sums of gray levels which is determined from the seven most significant bits of the image. The check-sum is embedded into the Least Significant Bits (LSBs) of pseudo-randomly selected pixel. Recently, the researchers have focused on wavelet based encryption schemes for image authentication. Some tamper localization schemes are proposed in wavelet domain. The techniques which uses transform domain are more complex and computationally expensive. Yet, they offer high degree of robustness against common image processing operations. Almost all the pixel-wise schemes proposed in literature encryption pixels sequentially, one pixel at a time. In these schemes, an image is scanned in a certain order to embed the encryption. The scan order may be public or secret. A neighborhood-dependent mapping function is used to map each pixel value to a desired logo bit. A special symmetry structure in the logo is used to authenticate the block content, while the logo itself carries information about the block origin (block index, the image index or time stamp, author ID). In block-based approach, the image is divided into sub-blocks and the encryption information is embedded into each and every block. Each individual block is authenticated by the successful retrieval of the encryption embedded in it. If the encryption of a particular sub-block is not retrieved successfully, then that sub-block alone is identified to be tampered and the remaining part of the image is authenticated. In these types of schemes, the localization resolution is based on the size of the sub-blocks. The smaller sub-block size is required to increase the detection resolution. But this will lead to higher encryption payload. The encryption is done for each block separately. Two versions of the algorithm have been proposed. In the private key version, the seven most significant bits of all

2. Z-TRANSFORM

In signal processing, the Z-transform converts a discrete time domain signal (a sequence of real numbers), into a complex frequency domain representation. The Z-transform is to discrete time domain signals what the Laplace transform is to continuous time domain signals. In mathematics and signal processing, the Z-transform converts a discrete time-domain signal, which is a sequence of real or complex numbers, into a complex frequency-domain representation.

$$Z[x_k] = \sum_{k=0}^{\infty} x_k z^{-k}.$$

It of time scale calculus. The z-transform was introduced, under this name, by Ragazzini and Zadeh in 1952. The modified or advanced Z-transform was later developed by E. I. Jury, and presented in his book *Sampled-Data Control Systems* (John Wiley & Sons 1958). The idea contained within the Z-transform was previously known as the "generating function method". The operation of a continuous-time system is described or modeled by a set of differential equations. On the other hand, a discrete-time system (or a sampled-data system) is described by a set of difference equations. The transform method employed in the analysis of continuous-time systems is the Laplace transformation. In a similar manner, the transform

used in the analysis of discrete-time systems is the Z-Transform. In other words, Z-Transform is the discrete counterpart of the Laplace Transform. Also, it may be thought as a generalization of the Fourier Transform for sampled-data signal as we shall see later on.We all know that the use of transforms in mathematical treatment to problems arising in certain applications is very important. The use of transforms has many advantages and because of these advantages, they are considered very powerful mathematical tools.

To determine the inverse Z-transform, it is necessary to know the RoC. RoC decides whether a given signal is causal (exists for positive time), anti causal (exists for negative time) or both causal and anti causal (exists for both positive and negative time) Different approaches to compute the inverse Z-transform Long division method When Z-Transform is rational, i.e. it can be expressed as the ratio of two polynomials P (z) and Q (z).

$$X(z) = \frac{P(z)}{Q(z)}$$

Then, inverse Z-transform can be obtained using long division:

Divide P (z) by Q (z). Let this be

$$X(z) = \sum_{i=-\infty}^{\infty} a_i z^{-i}$$

3. PROPOSED SYSTEM

The image from the data base is taken using a user friendly menu selection. The image is then read using imread function available in Matlab image processing tool box. Then the content to be water marked is also read and stored in a variable. The blockztrans sub routine is called to perform z transforms operation. After the water marked image is returned from the blockztrans function, both the original and water marked image is shown in the screen using imshow function. In addition to the above we show the encryption which we added to the image. The PSNR is calculated using the formula as shown given below.

$$\text{MSE} = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} \left[I(x,y) - I'(x,y) \right]^2$$

PSNR = 20 * log10 (255 / sqrt (MSE))

BLOCKZTRANS

In this file, we take z transforms for both the original image and water mark.And those pixels with the threshold greater than 250 are replaced with the z transform coefficients. Before transmitting it, an inverse z transform is obtained and transmitted.

DIGITALMARKS

This file is the one which decides the amount of encryption to be added in the host image. It takes into consideration about the size of the original image and the water mark image. Hence, the water mark is placed in all the parts of the host image.

In this project we design and development for the fragile encryption for digital image authentication by using the zeros of the z-transform. Digital image authentication is increasingly becoming more important with the tremendous development of the Internet. The ability of fragile encryption to detect changes in the encryptioned image to provide authenticity and integrity of the image makes it go a long way toward solving the image authentication problem. In contrast to a semifragile encryption, which only seeks to detect a predefined set of illegitimate distortions to the host image, a fragile encryption is designed to detect any change to the host image. Hence, a variety of fragile encryption methods has been proposed by embedding identifying information in the least-significant bits (LSBs) of the image. Unfortunately, these methods are somewhat unsecured as the use of LSBs could be easily detected and manipulated. However, the scheme was only able to localize distorted pixels altered in the five most significant bits. In our work, we propose a novel fragile encryption scheme in the z-transform domain. It does not modify the host image. Therefore, it is suitable for the application in which the modification of the image is not allowed. For example, satellite images cannot allow any modification on them because that will affect their precisions. Since PSNR obtained is more than 45 db, the water marked image looks as same as original image. The scheme is secure. By applying the technique of secret sharing, only the user who has the share image can retrieve the encryption. The scheme is robust and resistant to various attacks. The quantity of encryption added is more and still we have PSNR greater than 45db

4. RESULT ANALYSIS

In this project we introduce the new idea for encryption generally encryption is done by using the wavelet transform but in this project we prefer z-transform for fragile encryption for digital image authentication. The original image X is divided into non overlapping blocks of size N _ N, where N is an even positive integer. By viewing it row by row, each block can be expressed as a sequence of vectors $\{x_m\}$, m = 0; 1; . . . ; N-1, where $x_m = \{x_m[n]\}$, n = 0; 1; . . . ; N-1. We then perform the z-transform and obtain the zeroes, which are denoted as $\{z_{m;i}\}$ i = 1; . . . ; N-1, and m = 0; . . . ; N-1. We embed the encryption w by slightly perturbing the locations of the zeroes, where w is a binary sequence of N.

Fig.1.Encryptioned image

The encryption bits are randomly generated and the initial seed number is contained in a secret key file. A encryption signal of N bits long is embedded into every block, that is, one bit is embedded into every vector. To avoid the complex number computation, we embed the authentication encryption by slightly modifying the modulus of negative real zeroes, which are denoted by z_{nr}. As proven, since N is even, which is the case under most circumstances for natural images; there must be at least one real negative zero in the zero set of a pixel vector. Besides the negative real zero, there are (N=2)-1 pairs of complex zeroes for every vector (the number of complex zeroes would be less if multiple negative real zeroes exist). The small positive offset € determines the tradeoff between the fragility of the encryption scheme and the quality of the encryptioned image.After the encryption embedding process, we transform the zeroes back to the sequence using the inverse z-transform. We then obtain another vector x'_m, which is slightly different from the one before encryption. By applying the aforementioned process to all of the relevant blocks, we obtain the encryptioned image Y.

CONCLUSION

In this project, we have proved that a copyright protection scheme for grey scale images using z transforms. The scheme is suitable for gray images.
Furthermore, we still preserve the advantages of the previously proposed scheme, which are
(1) it does not modify the host image, and therefore is suitable for unchangeable images,
(2) it is secure because of the employment of secret sharing in z transform co efficient, and
(3) it is robust according to the experimental results, which shows the better accuracy rates.
(4). Also the coding efficiency is improved, and the PSNR obtained after the encryption is about 30db.

REFERENCES

[1] C.-S. Lu and M. H.-Y. Liao, "Multipurpose encryption for image authentication and protection," IEEE Trans. Image Process., vol. 10, no. 10, pp. 1579–1592, Oct. 2001.

[2] A. T. S. Ho, X. Zhu, and Y. L. Guan, "Image content authentication using pinned sine transform," EURASIP J. Appl. Signal Process., Special Issue Multimedia Security Rights Manag., vol. 2004, no. 14, pp. 2174–2184, Oct. 2004.

[3] M. Yeung and F. Mintzer, "An invisible encryption technique for image verification," in Proc. Int. Conf. Image Processing, Santa Barbara, CA, Oct. 1997, vol. 2, pp. 680–683.

[4] P. W. Wong, "A encryption for image integrity and ownership verification," presented at the IS & T PIC Conf., Portland, OR, May 1998.

[5] P. W. Wong, "A public key encryption for image verification and authentication," in Proc. IEEE Int. Conf. Image Processing, 1998, vol. 1, pp. 455–459.

[6] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical encryption for secure image authentication with localization," IEEE Trans. Image Process., vol. 11, no. 6, pp. 585–595, Jun. 2002.

[7] X. Zhang and S. Wang, "Statistical fragile encryption capable of locating individual tampered pixels," IEEE Signal Process. Lett., vol. 14, no. 10, pp. 727–730, Oct. 2007.

[8] E. C. Ifeachor and B. W. Jervis, Digital Signal Processing: A Practical

Approach. Wokingham, U.K.: Addison-Wesley, 1993.

[9] R. H. T. Bates, B. K. Quek, and C. R. Parker, "Some implications of zero sheets for blind deconvolution and phase retrieval," J. Opt. Soc. Amer. A, Opt. Image Sci.., vol. 7, no. 3, pp. 468–479, Mar. 1990.