www.ioirp.com

International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE)
ISSN: 2395-5619, Volume – 1, Issue – 3. May 2015

VIDEO WATER MARKING USING REVERSIBLE COLOR TRANSFORM AND DCT

RAJESHCHAKRAVARTHY.G.R
Electronics and Communication Engineering, Er.Perumal Manimekalai College Of Enginnering, Hosur, India
grkrish.rajesh@gmail.com

***Abstract*— Discrete Cosine Transform is used in the Multi Frequential data embedding in the video Water Marking Because we can Embed more amount of Data With security as compared with the Least Significant Bit method(LSB). The Least Significant Bit method(LSB method has got drawbacks such as easy data Loss by Intruder,Less data embedding, less security. So we are using the reversible color watermark image with 3D-DCT transform for the purpose of increasing security ,robust data embedding. We are going to be using Blum Blum Shub random pattern generator which is very much indeed a high security providing algorithm. The patterns generated with these pattern generators is quite tough to crack because it has got unique random code generation techniques which can be used to overcome disadvantages of previous LSB method of frequency embedding. We are also going to be using reverse color transformation technique to transform the water mark into a secrtet form.we are going to introduce otsus thresholding to prevent the congestion among the image in the process of secure image embedding We can also use advanced encryption standard for the purpose of secure data transfer. This can be used as alternative to cryptography sometimes due to high security features provided to this method with the help of 3d Dct ,Blum Blum Shub generator and Advanced Encryption Standard(AES) algorithm,The above method if used with Advanced Encryption Standard we can be able to transmit sensitive data wit lots of secrecy and thus can be Helpful in Transmitting Useful Sensitive data with multi frequential embedding using AES(Advanced Encryption Standard) We are going to use Matlab.**

I. INTRODUCTION

A. Context of research

Digital image authentication is increasingly becoming more important with the tremendous development of the Internet. The ability of fragile watermarking to detect changes in the watermarked image to provide authenticity and integrity of the image makes it go a long way toward solving the image authentication problem. Verification is done in the reverse order. Comparison with the logo indicates tampered blocks. In the public key version, the 7 MSBs are hashed using a fixed hash, XORed with the logo and then encrypted using a public key encryption method. The encrypted bit-stream is again inserted in the LSBs of the same block. During the verification process, first the hash of the 7 MSBs of all pixels in that block is calculated, XORed with the decrypted LSBs and the result is compared with the binary logo. The ability of this scheme to localize modifications is very satisfactory. The block size should be chosen so that the whole hash (128 bits) can be embeddedPrepare Your Paper Before Styling

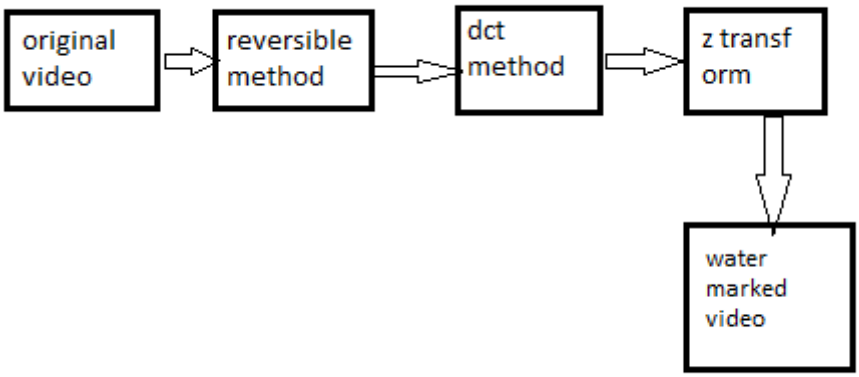
ADVANTAGES:

These advantages are:

1. Turning the differential or difference equations to algebraic ones, which are easier to solve?
2. The involved operation of convolution in the time domain is reduced to a multiplication operation in the transform domain.
3. The initial conditions are directly incorporated in the solution process and do not have to be separately incorporated.
4. The representation of a system in terms of the locations of poles and the zeros of the system transfer function in the complex plane.
5. The transient and steady state characteristics of a discrete system can be obtained by analyzing the poles and zeros of the system.

II. PROPOSED SYSTEM

In this project we design and development for the fragile watermarking 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 watermarking to detect changes in the watermarked 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 watermark, which only seeks to detect a predefined set of illegitimate distortions to the host image, a fragile watermark is designed to detect any change to the host image. Hence, a variety of fragile watermarking 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 watermarking scheme in the z-transform domain. The z-transform is a convenient yet invaluable tool for representing, analyzing, and designing discrete-time signals and systems. However, to our knowledge, this is the first time that this transform has been applied to digital watermarking. The locations of zeroes of the z-transform are very susceptible to any pixel value change. It has the advantage of easy implementation and pixel-wise sensitivity to external tampering. Moreover, it provides better data-hiding security protection than the normal LSBs check-sum fragile watermarking techniques.



Block diagram

A. ALGORITHM FOR WATERMARKING PROCESS

Watermarking process

1. The original image X is divided into non overlapping blocks of size NxN, where N is an even positive integer.
2. By viewing it row by row, each block can be expressed as a sequence of vectors.
3. We then perform the z-transform and obtain the zeroes.
4. We embed the watermark w by slightly perturbing the locations of the zeroes, where w is a binary sequence of N. The watermark bits are randomly generated and the initial seed number is contained in a secret key file. A watermark 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 watermark by slightly modifying the modulus of negative real zeroes.
5. After the watermark embedding process, we transform the zeroes back to the sequence using the inverse z-transform. We then obtain another vector X'
6. The output of this work is nothing but the Water marked image Y and the key generated k.

B. ALGORITHM FOR AUTHENTICATION PROCESS

Authentication process

1. In the authentication process, we need the watermarked image and the secret key to identify the watermark.

2. Let the watermarked image after passing through variant communication channels be Y'. The watermark sequence w is generated using the initial state number contained in the key.
3. The authentication process also starts by dividing the image into small blocks of size N x N. In every block, by applying the z-transform to every row, we obtain the zeroes.
4. We find the values of p from the hash functions and the watermarked image block after z transform/

III. RESULTS & ANALYSIS

In this project we introduce the new idea for watermarking generally watermarking is done by using the wavelet transform but in this project we prefer z-transform for fragile watermarking 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 watermark w by slightly perturbing the locations of the zeroes, where w is a binary sequence of N. The watermark bits are randomly generated and the initial seed number is contained in a secret key file. A watermark 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 watermark 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 watermarking scheme and the quality of the watermarked image.

After the watermark 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 watermarking. By applying the aforementioned process to all of the relevant blocks, we obtain the watermarked image Y.

In the authentication process, we need the watermarked image and the secret key to identify the watermark. Let the watermarked image after passing through variant communication channels be Ý. The watermark sequence w is generated using the initial state number contained in the key. The authentication process also starts by dividing the image into small blocks of size N*N.

IV. CONCLUSION & FUTURE WORK

A. 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 watermark is about 30db.

B. FUTURE WORK:

The project can be extended further with some other techniques like wavelet and DCT combined with z-transform for digital image authentication process. The computation time can be reduced by using high end processors. The same work can be extended for visible watermarking also.

Acknowledgment

My first and the foremost gratitude to almighty and my parents who showered the blessing and gave me the knowledge and strength to perform my work. I feel very pleasure to express my heart deep thankfulness to our chairman Er.E.Perumal B.E., Secretary Shri P.Kumar, A.M.I.E., Management Trustee Smt P.Malar, A.M.I.E., and our principal Dr. S.Chitra, Ph.D., for generously providing us with excellent facilities throughout the course of study and encouragement to do the project work. I hereby trace my thanks to Mr. M.Sahithullah, M.E., (Ph.D), Head of the Department of Electronics and Communication Engineering, for his encouragement and continued support or the successful completion o the project work. I express my gratitude and sincere thanks to our PG coordinator and guide Mrs.kavitha, M.E., Assistant Professor, department of electronics and communication who really a care taker and guided me in excellent way with in concern. With her fruitful suggestions and ideas i made this project a successful one. I express my sincere thanks to my friends, family members and all those rememberable personalities who had sacrificed their valuable time with me in the completion of this project work.

References

[1] C.-S. Lu and M. H.-Y. Liao, "Multipurpose watermarking 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 watermarking 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 watermark for image integrity and ownership verification," presented at the IS & T PIC Conf., Portland, OR, May 1998.

[5] P. W. Wong, "A public key watermark 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 watermarking 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 watermarking 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.

[10] R. Vich, z-Transform Theory and Applications. Dordrecht, The Netherlands: Reidel, 1987.

Authors Short Profile:

I am rajesh chakravarthy doing my M.E applied electronics. I aspire to enhance the existing process to make it effective in future I would like to be involved in many innovations driven research. I would like to thank almighty for all his blessings