International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.6, No.6, June 2017 DOI:10.15693/ijaist/2017.v6i10.1-5

Digital Image Protection Using Reversible Watermarking and Private Symmetric Key Encryption Technique

G. Balamurugan, V. Arulalan, K. Suresh Joseph

[1, 2] Department of Computer Science and Engineering, [3]Department of Computer Science,

[1, 2] Christ College of Engineering and Technology, [3]School of Engineering and Technology,

Pondicherry University,

Pondicherry-605010, India.

gbalamurugan1991@gmail.com, arulalanverrappan@gmail.com,

Abstract

Digital watermarking is a technique which has been recommended as a way to achieve digital protection. The aim of digital watermarking is to embed the data into the image without affecting the visual quality. The related work defines a robust block-based watermarking system on the singular value decomposition (SVD) and human visual system in the discrete wavelet transform (DWT) domain. The proposed method is considered to be a block-based scheme that utilizes the entropy and edge entropy as HVS characteristics for the selection of significant blocks to embed the watermark, which is a binary watermark logo. The proposal work includes reversible watermarking techniques and private symmetric key encryption
techniques are processed to maintain high imperceptibility and high robustness and also avoid the distortion caused by the geometric attacks. The experimental evaluation is also obtained for the proposed work.

Keywords: SVD, DWT, Digital Watermarking, block based scheme.

I. INTRODUCTION

Digital Watermarking is a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm. Cryptography provides a solution for the security issues. However, it does not completely address the relevant concerns because control of data distribution is lost when the encryption is removed. The best alternative solution to preserve the rights of the authors and ensure easy and fast access to internet resources is digital watermarking. This process of permanently embedding data into digital multimedia content without degradation, such that this watermark can resist any extraneous operation. The watermark can be visible or invisible; invisible watermark are the most commonly employed. The protection and enforcement of intellectual property rights for digital media has become an important issue. Establishing block based image watermarking techniques is used because of their advantages, one of which is the ability to process each block individually. The basic of this technique is to embed the watermark into the selected blocks, which are the blocks or regions bearing the basic character information of the image, such as the texture and edges. A human visual system (HVS) is adopted as a good method to select the blocks and to improve the robustness and imperceptibility by exploiting the characteristics of the block, such as entropy and edge entropy.

II. RELATED WORK

A novel watermarking method based on the singular value decomposition (SVD) and discrete wavelet transform (DWT) domain is said to be an efficient scheme that utilizes the entropy and edge entropy as HVS characteristics for the selection of significant blocks to embed the watermark, which is a binary watermark logo. The blocks of the lowest entropy values and edge entropy values are selected as the best regions to insert the

watermark. After the first level of DWT decomposition, the SVD is performed on the low-low sub-band to modify several elements in its U matrix according to predefined conditions.

III. DRAWBACKS IN THE RELATED WORK

In order to overcome the drawbacks such as less imperceptibility and less robustness present in the related work, an efficient proposed system is used to maintain the digital watermarking.

IV. PROPOSED WORK

This proposal includes reversible watermarking techniques and private symmetric key encryption techniques are processed to maintain high imperceptibility and high robustness and also avoid the distortion caused by the geometric attacks. The main advantages of the proposal are to provide High Imperceptibility and High Robustness.

V. MODULES

The proposed work consist of three main modules for the processing

I. Embedding process
II. Key generation using Symmetric key encryption
III. Extraction process.

A) Embedding process

In this the proposed system, the host image block is selected using SVD and DWT. The message content for watermark is encrypted using symmetric private key and then the encrypted message is embedded in image using reversible watermarking.

B) Extraction process

In this extraction process, the watermarked image is processed by reversible watermarking, then the encrypted message is obtained from the image and using the symmetric key decryption process original message is extracted.

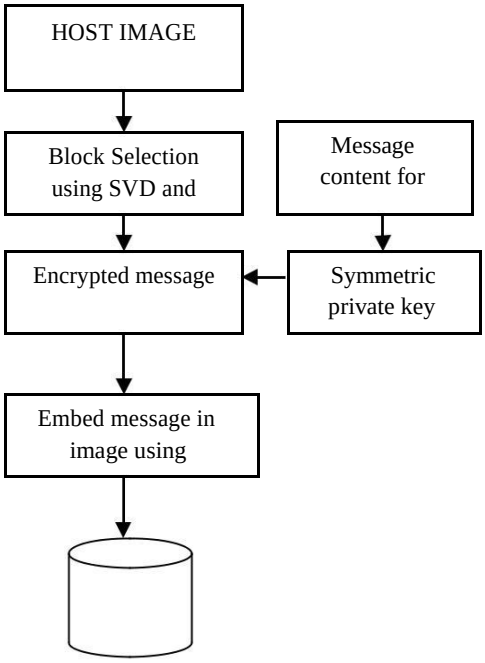

Figure1: Embedding of watermarking

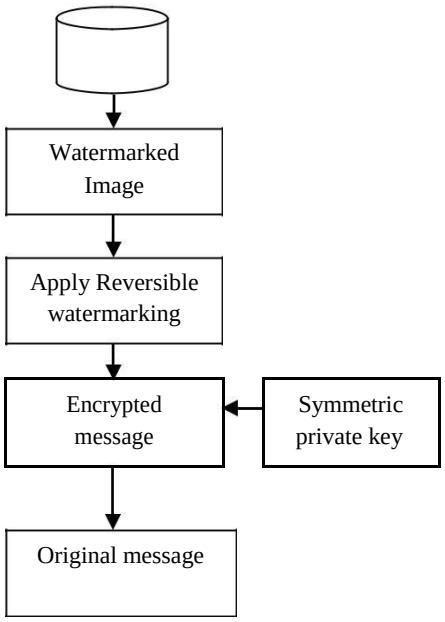

Figure 2: Extraction process using Reversible watermarking

VI. WORKING OF REVERSIBLE WATERMARKING

A) WATERMARKED EMBEDDING PROCESS

a) Step 1: The original image (I) is divided into sub-blocks B^k, where k =1, 2... N, N =Ww X Wh, Ww and Wh are the width and height of the watermark, respectively.

b) Step 2: Two-level wavelet transform is applied to each sub-block. We select coefficients in the low frequency part to enhance robustness against additive noise, filtering, and JPEG compression.

c) Step 3: Perform SVD on the low frequency wavelet coefficient of each block to generate SVs (Sk).

d) Step 4: Watermark bits are embedded by quantization using the reversible watermarking algorithm; the SV's of wavelet approximate coefficients are selected to be quantized since the first Sv's are most robust to geometric distortion.

e) Step 5: Apply SVD calculation to obtain updated SVs for the host signals

f) Step 6: the IWT is performed to obtain the watermarked host medical image (I*)

$$S_w^k = \begin{cases} S_a^k + 1 - \mathrm{mod}(S_a^k, 2), & \text{for } E(i,j) = 1, \\ S_a^k + 1 - \mathrm{mod}\left((S_a^k + 1), 2\right) & \text{for } E(i,j) = 0, \end{cases}$$

B) WATERMARKING EXTRACTION PROCESS

a) Step 1: The watermarked host medical image (I) is partitioned into sub-blocks B^k, where k =1, 2... Ww X W_h.

b) Step 2: Two-level wavelet transform is performed to each sub block B^k . The approximate coefficients are selected for SVD calculation.

c) Step 3: Perform SVD on the low frequency of each block to generate SVs (S^k).

d) Step 4: The SVs (S^k) is then normalized according to

e) Step 5: The final message is obtained

VII. KEY GENERATION PROCESS FOR PRIVATE SYMMETRIC KEY

Four steps cipher algorithm is proposed to operate on block and stream of bits/bytes of plain text or image. The stream cipher algorithms combine the bits/bytes of plain text I_p = [I1, Ii, In] with a secret four bit key Ke = [k1...k4] issued from the source. The secret four bit key Ke, is used for encryption and decryption hence it is a part of private symmetric key encryption techniques. Thus, bits/bytes of cipher text Ie = [Ie1... Iei, Ien]. The specialization of the algorithm resides on four bit key and algorithm.

The four steps cipher algorithm consists of four different operations for encryption and decryption hence the user cannot decrypt the data even though he knows the encryption algorithm with the key that verifies the reliability and confidentiality. The data Ip is encrypted by bitwise division and multiplication with two reverse shift operations, hence the algorithm is very simple in nature with two reverse operations making it more secure, cyclic redundancy check (CRC) in receiving ends is easier and it works well for a small amount of data.

VIII. PARAMETER EVALUATION

To provide the reliability and quality of service to the watermarked image, the performance of watermarking is calculated, which measured in terms of robustness and perceptibility. There are two methods of calculating the performance measure.

Mean Square Error (MSE): It is the simplest function to measure the perceptual distance between watermarked and original image. MSE can be defined as:

$$MSE = \frac{1}{n}\sum_i^n (I' - I)^2$$

Peak Signal to Noise Ratio (PSNR): It is used to measure the similarity between images before and after watermarking.

$$PSNR = 10 \log_{10} \frac{maxI}{MSE}$$

Normal Correlation values (NC) compares the input and output image and provides the result. If NC value is „1" concludes that no attack occurred on the image, else if NC value is less than "1"concludes an external attack occurred on the image. Value ranges between "0" to "1" gives tampering or the distorted factor of the image. For the less value of NC declares more amount of distortion on the image.

SEQUENCE	PSNR	NC
1	44.2012	1
2	45.119	1
3	42.5848	1
4	51.2546	1
5	50.8055	1

Table 1: PSNR and NC for DWT-SVD without attack

PSNR	ATTACK	NC
44.2012	MEDIAN	1
45.119	NOISE	0
42.5848	ROTATION	1
51.2546	SHEAR	1
50.8055	CROP	1
46.6372	MEDIAN	1

Table 2: PSNR and NC for DWT-SVD with attack

IX. EXPERIMENTAL IMPLEMENTATION

Figure 3: Main Menu

Figure 4: Embedding Process

Figure 5: Extraction Process

CONCLUSION

The proposed system is used to achieve high robustness and high imperceptibility, reversible watermarking and symmetric key cryptography technique. Several characteristics were employed to achieve high-level grades for the watermarking requirements and maintain the trade-off between them. Initially, blocking was used to divide the image into blocks. Then, only a portion of these blocks were selected to include the watermark; this selection ensured that the embedding process would affect specific regions of the image. The HVS characteristics of entropy and edge entropy were used to select the low informative blocks as the best embedding regions. The scheme employed the properties of a DWT and SVD. These methods aimed to provide high robustness by selecting the most robust regions with an emphasis on maintaining non-noticeable distortions, in other words, to maintain imperceptibility.

ACKNOWLEDGMENTS

I deliver my truthful thanks to Dr. A.Ravichandran M.E., Ph.D., M.I.S.T.E., M.I.E., Director (Christ College of Engineering and Technology & Christ Institute of Technology) for providing the wonderful opportunity and kind guideline for research article preparation

REFERENCE

1) Gerhard, C., Setyawan, I., Lagendijk, R.: 'Watermarking digital image and video data', IEEE Signal Process. Mag., 2000, 17, (5), pp. 20–46
2) Chang, C., Lin, P., Yeh, J.: 'Preserving robustness and removability for digital watermarks using sub sampling and difference correlation', Inf. Sci., 2009, 179, (13), pp. 2283–2293
3) Huang, C., Wu, J.: 'Fidelity-guaranteed robustness enhancement of blind-detection watermarking schemes', Inf. Sci., 2009, 179, (6), pp. 791–808
4) Liu, K.C., Chou and C.H.: 'Robust and transparent watermarking scheme for color images', IET Image Process., 2009, 3, (4), pp. 228–242
5) De Vugt, F.: 'Quantization-watermarking methods for digital audio', 2001
6) Ruanaidh, J., Pun, T.: 'Rotation, scale and translation invariant digital image watermarking'. Proc. IEEE Int. Conf. Image Processing, 1997, pp. 536–539
7) Makbol, N.M., Khoo, B.E.: 'Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition', AEU-Int. J. Electron. C, 2013, 67, (2), pp. 102–112
8) Chang, C., Lin, C., Tseng, C., et al.: 'Reversible hiding in DCT-based compressed images', Inf. Sci., 2007, 177, (13), pp. 2768–2786
9) Cox, I., Kilian, J., Leighton, F., et al.: 'Secure spread spectrum watermarking for multimedia', IEEE Trans. Image Process., 1997, 6, (12), pp. 1673–1687
10) Li, Q., Cox, I.: 'Using perceptual models to improve fidelity and provide resistance to volumetric scaling for quantization index modulation watermarking', IEEE Trans. Inf. Forensics Sec., 2007, 2, (2), pp. 127–139
11) Aslantas, V., Ozer, S., Ozturk, S.: 'Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms', Opt. Commun.,2009, 282, (14), pp. 2806–2817
12) Li, L., Yuan, X., Lu, Z., et al.: 'Rotation invariant watermark embedding based on scale-adapted characteristic regions', Inf. Sci., 2010, 180, (15), pp. 2875–2888
13) Lin, T., Lin, C.: 'Wavelet-based copyright-protection scheme for digital images based on local features', Inf. Sci., 2009, 179, (19), pp. 3349–3358
14) Maity, S., Kundu, M., Das, T.: 'Robust SS watermarking with improved capacity', Pattern Recognit. Lett., 2007, 28, (3), pp. 350–356
15) Lai, C.C., Tsai, C.C.: 'Digital image watermarking using discrete wavelet transform and singular value decomposition', IEEE Trans. Instrum. Meas., 2010,59, (11), pp. 3060–3063.