www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 19936-19940
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.14

Hybrid Technique Based Blind Digital Image Watermarking

Shubhangi Pande[1], Santosh Varshney[2]
[1]M.Tech, IV Semester, Department of CSE,
LNCT, Indore (M.P.), India
Shubhangi.shanu@gmail.com
[2]Asst. Professor, Department of CSE,
LNCT, Indore (M.P.), India
varshneysantosh.25@gmail.com

Abstract: Nowadays Internet is an excellent priority base source for everyone for sales and distribution and everything for digital assets, but because of this world wide sharing of digital information now there is an issue of copyright compliance and content management can be a challenge for us. Now a digital information can be used everywhere very easy way with or without using consent. Digital image Watermarking is an ultimate solutions that can add an extra security layer of protection for a digital images. In a digital image watermarking technique an image or an object embedded with some information carrying watermark, this object may be audio or video. These watermarking embedded techniques based on DWT –Twin Encoding technique drive the benefits from random sequence generated by Arnold and Chaos transformations. The proposed system before sending the multimedia data it apply the composite partition algorithm, watermark optimization techniques and the resulting file is Encrypted using RSA algorithm with public key and send it to the client side. Simulation result shows the performance of watermarking of image against different attacks. In the end, the performance of the proposed technique will be measured on the basis of PSNR, and NCC.

Keywords: DWT, DCT, Digital Image Watermarking, Twin encoding, RSA, Arnold Transformation, Chaos Transformation, PSNR, NCC, etc.

1. Introduction

With the rapid enhancement of digital information technology the data distribution at worldwide level is become very easy. This fastest development also effected on the security issue of data from the other facts like counterfeiting, piracy and malicious maniple. For the protection of data many number of mechanism are used, digital image watermarking is one of them. Watermark-It is a label, a tag, an information container which inserted or embedded into image data to make original image data secure from illegal manipulation and distribution. Embedded information can be visible or invisible to other world. Digital image watermarking compress the main feature like it doesn't make any effect on the quality of image with having a strong concern about the geometric and non-geometric shape included in an image also known as robustness of watermarking. Digital image watermarking can de describes in following domain scheme; spatial domain scheme, transform domain scheme and feature base watermarking scheme. In the spatial domain scheme the information tagged in a specific pixel of digital image,

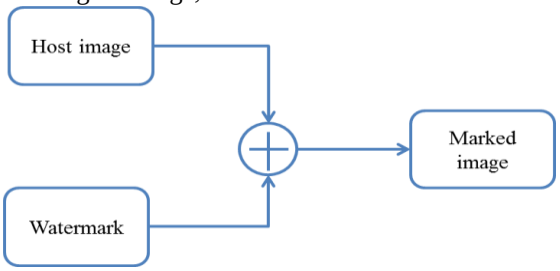

Figure 1: Spatial Domain Watermarking

While in case of transform domain scheme, first image transfer into frequency domain then information tagged to its frequency coefficient. In the both watermarking technique the transform domain scheme is more complex but more secure against different attacks

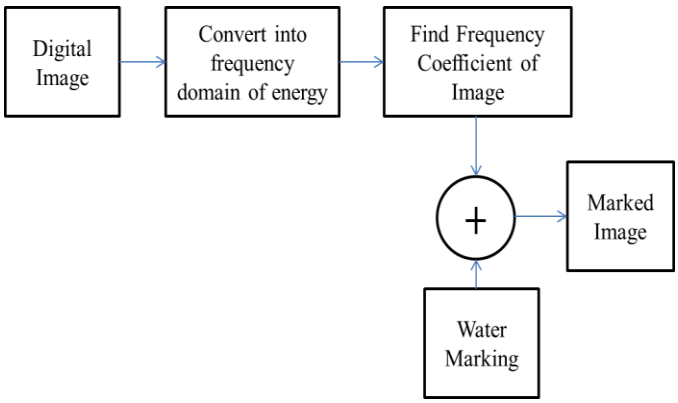

Figure 2: Transform Domain Watermarking

In the feature base watermarking, first we select the main feature of an image as the main feature of an image having high invariance to distortion so it can be used as key to set watermark of image with a constraint that it will not make any effect in the geometric and non-geometric feature of an image.

2. LITERATURE REVIEW

Deepa et.al, in this paper, proposes a method for watermarking on still image based on the concept from wavelet based data fusion. This technique is highly robust to compression and additive noise factor of an image, also beneficial and effective when the images are almost completely destroyed, yet it can be extracted fairly accurately. Propose method is also quite flexible to moderate linear mean ltering. It uses the discrete wavelet transform for the independent processing of the resulting components like the human eye [1].

Pratibha et.al, this paper are develop a technique based on multi-bit watermark and embedded it into a low frequency band

of cover image with the help blending technique. At the time of tagging the watermark image, the image get scatter within original image because of scaling factor of alpha blending technique. Develop technique can embed the invisible watermark into the digital image using alpha blending technique , and which can be recover by extraction technique. Its Experiment results define that the quality of the watermarked image are mainly dependent on the scaling factor [2].

3. DISCRETE COSINE TRANSFORM (DCT) WATERMARKING

The DCT technique is used to convert frequency domain signal into time domain signal. For using time domain signal, an image is easily split into pseudo frequency bands and in this work watermark techniques inserted into middle band frequencies since as discussed in all frequency domain watermarking techniques, there is a conflict among robustness and transparency. The Discrete Cosine Transform is a Fourier related transform similar to Discrete Fourier Transform but using only real numbers. The Discrete Cosine Transform are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since Fourier transform of real and even function is real and even).

4. DISCRETE WAVELET TRANSFORM (DWT) WATERMARKING

The Wavelet transform has been widely studied in signal processing in general and image compression in particular. The Two dimensional Discrete Wavelet Transform scheme is used to decompose the image into four sub bands namely LL, LH, HL & HH.

LL- Low frequency band
LH- Horizontal high frequency band
HL- Vertical high frequency band
HH- Diagonal high frequency band

The Wavelet coding techniques are especially suitable for applications where scalability and tolerable degradation are important.

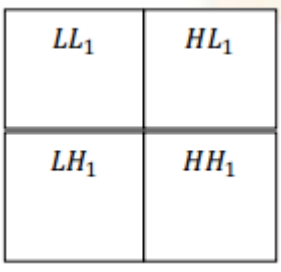

Figure 3: Single level Decomposition using Discrete Wavelet Transform

5. RIVEST-SHAMIR-ADLEMAN (RSA) ALGORITHM

The four steps of RSA algorithm are key generation method, key distribution encryption and decryption. For the sender encrypts his image using public key (e, n) and the receiver decrypts the image using the private key (d, n) where 'e' is

$$1 < e < ((p-1) \times (q-1)) \quad (1)$$

and e ,n are co-prime. p and q are assigned co-prime numbers. Firstly the image data is converted into the integer m such that $0 <= m < n \text{ and } gcd(m, n) = 1$. The cipher text 'c' is computed by the equation c=me (mod n) where n is the product of p and q.

The receiver recovers integer m by the private key exponent d' by performing m=cd mod (n).

The algorithm has been explained in details below in subsections E and F. In subsection E, embedding algorithm is presented. The watermark is extracted in the reverse way which is given in subsection F.

6. ARNOLD TRANSFORM

The Arnold transformation, it is also called cat mapping, is a tool changing one matrix into another. A be a NN matrix, a point (i, j) can be shifted to another point (i', j') by equation:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} (mod\ N) \quad (2)$$

It is known that the Arnold transform system works well in applications for encrypting images. For an $N \times N$ matrix image, Arnold transform is given by equation (2) where (a, b) and (x, y) express the pixel coordinates of the original and encrypted images, respectively. With the periodic boundary treatment, the image encryption using iterations of the Arnold transform may be written as:

$$I(x, y)^{(k)} = ID(a, b)^{(k-1)} (mod\ N) \quad (3)$$

Where, $k = 1,2, \ldots N \text{ and } I(x, y)0 = I(a, b)$. The Arnold transform matrix is given as in (6) and I is an $N \times N$ image field. The encrypted image may be inverted by applying the inverse of the Arnold matrix times as follows:

$$I(a, b)^{(k)} = ID^{-1}(x, y)^{(k-1)} (mod\ N) \quad (4)$$

Where $(x, y)0$ is the pixel of the encrypted image. An original image may reappear after iterations, depending on the size of the given image. The periodicity depends on the size of the images [10].

After certain number of Arnold transformation, matrix A reappears. Denote the number of Arnold transformation when A reappears as period. In our experiments, Arnold transformation is performed on 128×128 matrices, and period=96. After Arnold transformation, security and robustness of our algorithm is increase

7. RESULTS

The proposed idea will be implemented in MATLAB software which is extensively utilized in all regions of applied mathematics method. The system block diagram of different transform based watermarking technique for proposed work is

DOI: 10.18535/ijecs/v6i1.14

shown in Fig. 4. The methodology of proposed work is given as:

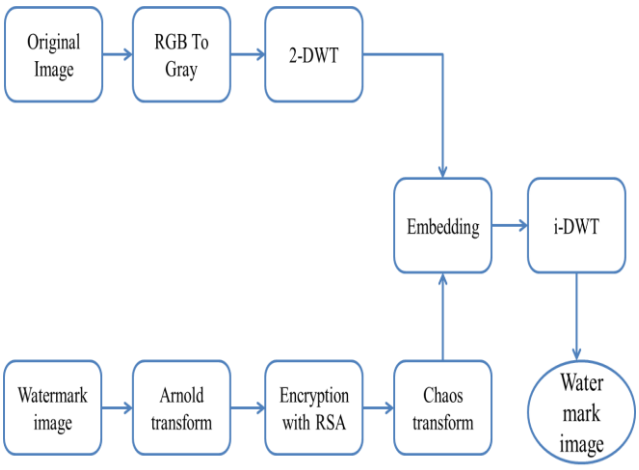

Figure 4: Block Diagram Embedded Watermarking

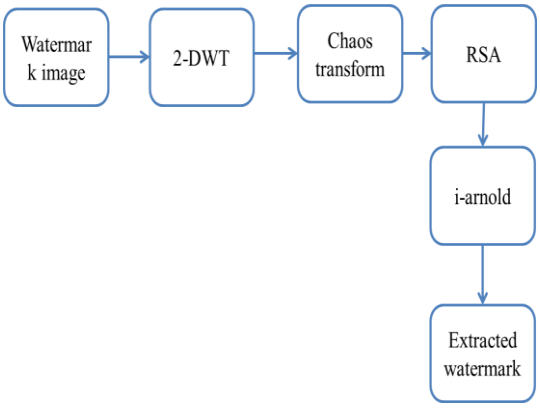

Figure 5: Block Diagram of Watermark Extraction

For the performance of wavelet transform, Chaos transform and Arnold transform based watermarking techniques shown in Fig. 5. The proposed algorithm it is assumed that the dimension of the cover image I is N x N matrix. First step embed the watermark in a cover image or host image by using watermark embedding techniques and then the watermark will be extracted using extraction algorithm and RSA algorithm. For the robustness of the algorithm will be measured by applying attacks on watermarked image and then with the help of performance parameters NCC and PSNR values the robustness of the extracted logo will be evaluated.

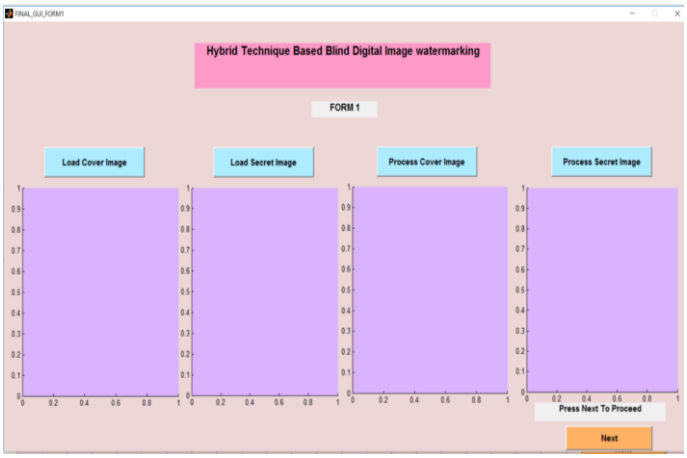

Figure 6: GUI for Inputs Data

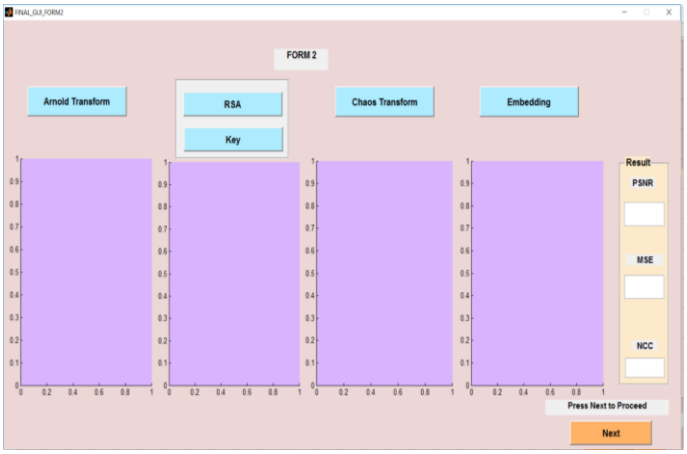

Figure 7: GUI for Embedding Process

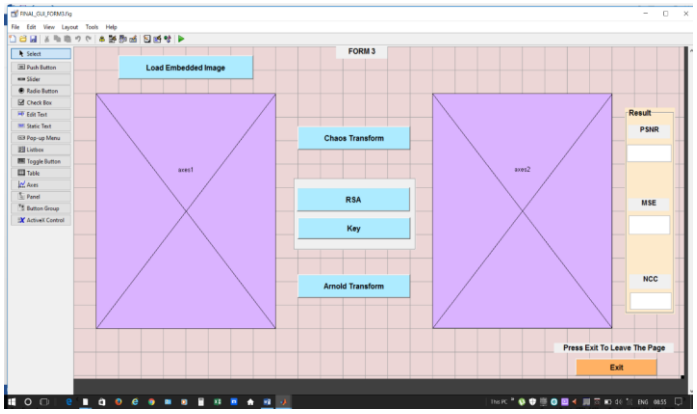

Figure 8: GUI for Extraction Process

Figure 9: Cover Image

Figure 10: Watermark

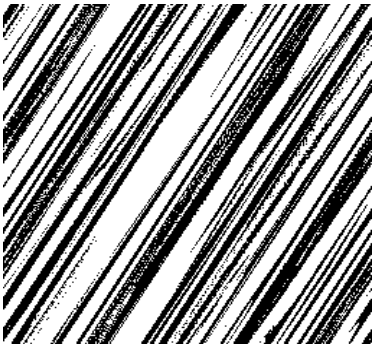

Figure 11: Arnold Transform

Figure 12: RSA encryption

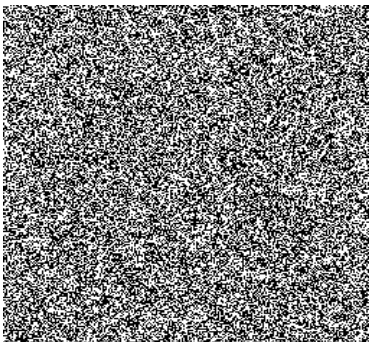

Figure 13: Chaos Transform

Figure 14: Embedded Image

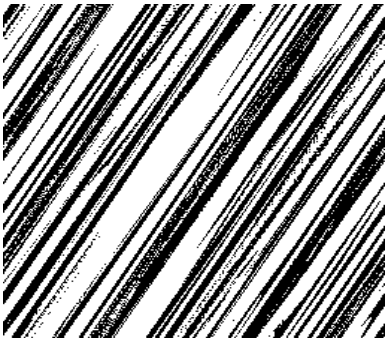

Figure 15: Inverse Chaos Transform

Figure 16: RSA Decryption

Figure 17: Inverse Arnold Transform

Experimental results are examine by PSNR, MSE and NCC parameters. PSNR stands for peak signal to noise ratio. Larger the value of PSNR, better the quality of image or we can say that smaller the value of PSNR, larger the difference between images. PSNR value is accepted it is above 30dB. MAE is the mean absolute error. Mae measure the difference between an original watermark and corresponding extracted one. Lower the value of MAE means more robust. NCC stands for normalized cross correlation. The value of NCC is in between [0, 1]. Larger the value of NCC, similarity between images is more. Generally, its value of greater than 0.7500 is accepted.

In the proposed method, we are using Gain Factor in embedding process, which results that it increases PSNR value which include RSA algorithm also. This means that, security increases as compared to the previous method which uses Arnold and chaos transformation only. One of the main advantage of gain factor is, at the particular value of gain factor, the PSNR value is same for any image. It means, result does not depend on image type, rather it depends on gain factor value. The result of proposed method for some images are given below:

Table 1: Experimental Results in Terms of Performance Parameters

Gain Factor	*Lena gray*			*Camera man*			*Mandril gray*			*Lena color*			*Mandril color*		
	PSNR	MSE	NCC	PSNR	MSE	NCC	PSNR	MSE	NCC	PSNR	MSE	NCC	PSNR	MSE	NCC

0.1	74.1514	0	1.0000	74.1514	0	1.0000	74.1514	0	1.0000	74.1514	0	1.0000	74.1514	0	1.0000
0.5	60.1720	0	1.0000	60.1720	0	1.0000	60.1720	0	1.0000	60.1720	0	1.0000	60.1720	0	1.0000
1	54.1514	0	0.9999	54.1514	0	0.9999	54.1514	0	0.9999	54.1514	0	0.9999	54.1514	0	0.9999
1.5	50.6296	0	0.9999	50.6296	0	0.9999	50.6296	0	0.9999	50.6296	0	0.9999	50.6296	0	0.9999
2	48.1308	0	0.9999	48.1308	0	0.9999	48.1308	0	0.9999	48.1308	0	0.9999	48.1308	0	0.9999
2.5	46.1926	0	0.9998	46.1926	0	0.9998	46.1926	0	0.9998	46.1926	0	0.9998	46.1926	0	0.9998

8. Conclusion

Watermarking technique using DWT has been completed successfully. The security has been added with multiple encryption techniques. The higher PSNR has been achieved for embedded image using these techniques. The use of multiple encryption techniques reduced the dependency of secrete image histograms. The secrete image has recovered at the receiver side faithfully.

References

[1] Deepa Kundur and Dimitrios Hatzinakos "A Robust Digital Image Watermarking Method using Wavelet-Based Fusion"

[2] Pratibha Sharma,Shanti Swami" Digital Image Watermarking Using 3 level Discrete Wavelet Transform", Conference on Advances in Communication and Control Systems, 2013.

[3] M. Calagna, H. Guo, L. V. Mancini and S. Jajodia, "A Robust Watermarking System Based on SVD Compression", Proceedings of ACM Symposium on Applied Computing (SAC 2006), Dijon, France, pp. 1341-1347, 2006.

[4] Dr. M. A. Dorairangaswamy, "A Robust Blind Image Watermarking Scheme in Spatial Domain for Copyright Protection", International Journal of Engineering and Technology vol. 1, no.3, pp. 249 - 255, August 2009.

[5] S. Murty. P, M. U. Bhaskar, P. N. Babu and P. R. Kumar, "A Semi-Blind Reference watermarking Scheme Using DWT-DCT-SVD for Copyright Protection", International Journal of Computer Science & Information Technology (IJCSIT) vol. 4, no 2, pp. 69-82 April 2012.

[6] F. Cayre, C. Fontaine and T. Furon, "Watermarking security: theory and practice", Signal Processing IEEE Transactions vol. 53, no. 10, pp. 3976–3987, Oct. 2005.

[7] Ms. Kapre Bhagyashri S and Mrs. Joshi M.Y.,"Robust Image Watermarking based on Singular Value Decomposition abd Discrete Wavelet Transform", IEEE,pp.337-341, 2010.

[8] Nidhi H. Divecha and N.N.Jani, "Image Watermarkin Algorithm using DCT-DWT-SVD", Proceedings published by International Journal Of Computer Applications (IJCA), pp.13-16, 2012.

[9] Satyanaryana Murty,M.Uday Bhaskar,P.Rajesh Kumar,"A Semi-Blind Reference Watermarking Scheme Usind DWT-DCT-SVD For Copyright Protection",International Journal Of Computer Science and Information Technology(IJCSIT), Vol 4,No 2, April 2012.

[10] Yang B.and Deng B., "Steganography In Gray Images Using Wavelet", Nanjing University of Post and Communication Technology, 17(7): 60-72, 2010.

Author Profile

Ms. Shubhangi Pamde, received the BE degree in Computer Engineering from Mandsaur Institute of Technology, Mandsaur in 2007 and Presently she is pursuing M.tech in Computer Engineering from LNCT, Indore (MP), India.

Mr. Santosh Varshney, received the BE and M.tech degree in Computer Engineering Govt. engineering college, Bhopal and ICSEI, DAVV in 1993 and 1996 respectively. Presently he is working as an Assistant Professor in CS/IT dept. at LNCT, Indore (MP), India.