International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 – 6435(Online), Volume 1, Issue 1, Oct 2013)

Image Security through DWT &SVD based Watermarking and masking with Encryption

Tapas Bandyopadhyay[1], B Bandyopadhyay[2], B N Chatterji[3]

[1]*Scientist F, STQC, Kolkata-91*
[2]*Professor, C.U.*
[3]*Ex Prof IIT, Kharagpur*

Abstract-- **The rapid growth in the digital technology, image processing tools and communication revolution through Internet has made the reproduction of digitally created artifacts simple and within reach very easily. This new trend has several advantages in terms of flexibility, cost effectiveness, convenience etc., but at the same time, also raised some serious concerns in actual real life situation. Information security is an evolving phenomenon and no single technique seems sufficient enough to provide security of the images in the internet environment [1][12]. Encryption and digital watermarking techniques may be incorporated together in digital right management to achieve better security [2][3]. These two technologies are complimenting each other, and the increased security of the digital artifacts can be achieved by using benefits of the both. Encryption transforms the original digital contain into human unreadable format and watermarking leaves the digital object intact and recognizable with a permanent embedded tag of user specific information or logo embedded into it[7]. To hide the secret user specific information in the form of watermark it is encrypted using secret key based congruently generated pseudorandom number and then bitxoring to generate the encrypted watermark. The encrypted watermark is embedded in the host image using DWT and SVD based techniques and the watermarked image is further encrypted using key hashed based encryption techniques. This will prevent man in the middle attack by intercepting the watermarked image by the malicious attacker who may try to remove or distort the watermark and use it for malicious purpose. This technique makes the image human unreadable format and reduced in size while distribution and the user specific information is encrypted and permanently tagged with the host image through watermarking for authentication purpose [11]. The experimental results demonstrate the high robustness of the proposed algorithm to various image processing attacks like noise additions, rotations, cropping, filtering, compression etc.**

Keywords-- **watermarking, encryption, entropy, pseudorandom number, PSNR, normalized cross correlation (NCC), Normalized Hamming Distance (NHD))**

I. INTRODUCTION

To cope with the challenges of information security threats in the internet environment counter measures are needed to prevent the illegal copying, forgery and distribution of multimedia digital content in the form audio, images text, video etc. Different techniques like digital watermarking, steganography, cryptography etc. are being used across the globe. The digital watermarking schemes have been proposed in the last decade, where a small amount of imperceptible secret information is embedded into the digitalartwork t, which can be extracted at a later stage for copyright assertion [2].The encryption techniques converts the digital information in to non-intelligent form, only the authorized person with proper key can decipher the digital content again in the intended intelligent form. Any single technique may not provide sufficient security to the digital content in the evolving situation of internetenvironment with smart people around the world enhanced and equipped with different attacking tools. In order to face the challenges of security threat of the digital content in a effective and efficient way a combination of different techniques and approaches may be In order to achieve increased security of the digital artifact like artwork or image.The invisible embedded watermarks carries some secret information that may be considered attributes of the cover host image such as copyright 4][5][9].The encryption process scrambles and mask the data in order to make them unintelligible to any unauthorized user who might want to intercept them for malicious purposes.The conventional cryptographic system permit only valid key holders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission [1,3,5]. The cryptography mechanisms protect the digital content during transit only after decryption of the transmitted digital content no control is there to prevent copying of the content.

Digital watermarking is used for protecting intellectual property rights (IPR) of digital multimedia data by a process of embedding a secret message code to the content or digital artifact data to be protected. Thissecret code remains permanently embedded in the data even after decryption [7][8]. This code remains invisible but can be extracted on demand to verify the authenticity of ownership of the media file. To enhance the security of the user specific secret information in the networked multimedia system the watermark can be first encrypted using a secret key. The encrypted watermark is then watermarked in the host image and transmitted to the intended user. The invisible watermarking is images in the internet arena can be enhanced by this technique. The types of protection systems involve the embedded in the original image in the wavelets domain using and using SVD based technique [8][10]. The imperceptibility quality of the images is quite good after the embedding of the watermark. The security of the use of both encryption and authentication techniques. We have described a technique of combined effect of protection of digitalmedia through digital watermarking and cryptographic authentication techniques.

II. Background

2.1 DWT decomposition of image

The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.

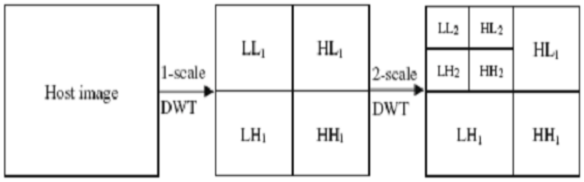


Figure 1:wavelet decomposition of image

2.2 Singular Value Decomposition of image:

Singular Value Decomposition (SVD) is a numerical technique for diagonalizing matrices in which the transformed domain consists of basis states that is optimal in some sense [4[7]]. The SVD of an N x N matrixA is defined by the operation:$A = U S V^T$

Where U and V are NXN unitary and S is NXN a diagonal matrix. The diagonal entries of S are called the singular values of A and are assumed to be arranged in decreasing order $\sigma i > \sigma i + 1$.

III. Watermark Embedding Scheme

The user logo watermark information is embedded to the host image as a proof of ownership, in case of any dispute the author of the original image can prove his ownership. The watermarking scheme is so designed that the visual distortion of the host image is not much disturbed as well as the robustness of thewatermark is a good enough. The watermarkingembedding scheme is depicted in the block diagram figure 2.0.

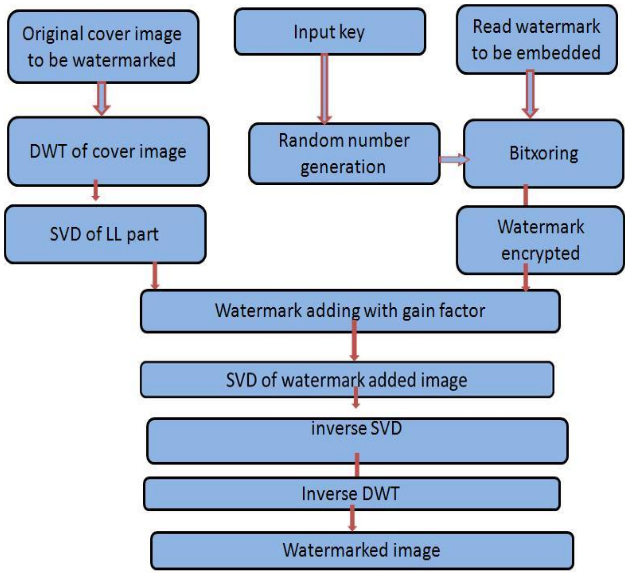


Figure 2.0: Embedding scheme of the encrypted watermark

Step1: Read the image to be watermarked

Step2: Apply DWT to decompose the cover host image into four non-overlapping multi-resolution sub bands: LL1, HL1, LH1, and HH1.

Step 3: Apply SVD decompose of the LL band.

Step 4 Read the watermark to be embedded in the host image

Step 5 Input the Key for pseudorandom number generation

Step 6 Bitxoringto encrypt the watermark

Step 7 Singular (S) value of the host image is modified with the watermark and gain factor

Step 8 Apply SVD decompose of the modified image

Step9 Calculated the Inverse SVD

Step 10 Inverse DWT to get the watermarked with encrypted watermark

IV. Encryption Scheme Of The Watermarked Image

The proposed image encryption scheme exploit the security behavior of the hash function for key hashing and wavelet transform of the cover image. The hash value (MD5) of the key file is generated and stored as text file. The secure one way functions are very important tool for checking integrity, privacy and authentication in cryptographic application. Figure 2 depicts the encryption scheme for the encryption of the watermarked image.

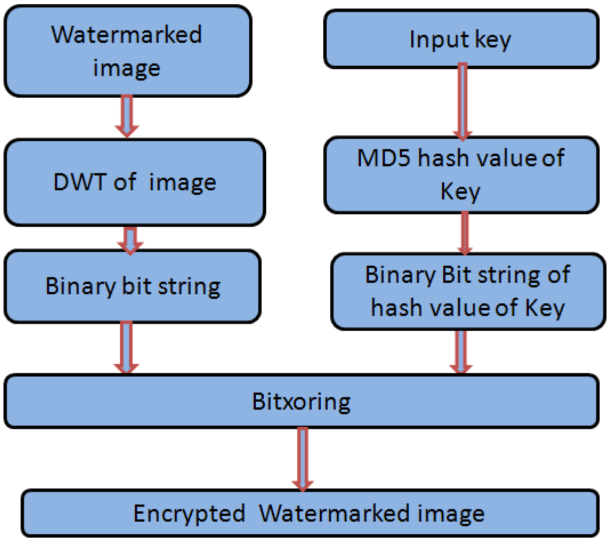


Figure 2: Scheme for Encryption of the watermarked image

The secret key value is fed into the openssl tool to generate the MD5 hash of the key value.

Step 1. The MD5 hash value is then concerted to binary string.

Step2 Load the image to be encrypted.

Step 3 Calculate the wavelet transform of the image.

Step 4 Convert the binary string of the wavelet components

Step 4 Expand the key to match with the image size.

Step 5 Bitxoring the key and binary string of the wavelet coefficient.

V. Experimental Results

The watermark is first encrypted with key and the pseudorandom number using the algorithm and the same is embedded in the host image in wavelet domain. The MD5 hash value of the key file is generated using OpenSSL tool. The encryption and decryption algorithm is developed using Matlab 7.0 programme. The test images are used for the experimental purpose.

A good encryption scheme should be robust against all kinds of cryptanalytic, statistical and bruteforce attacks. Some experimental results are given in this section to demonstrate the efficiency of ourScheme. All the experiments are performed on a laptop PC with Intel® Pentium® processor, 1.3GHz CPU, 1.24 GB RAM withWindows XP professional Edition. Table1, Table2 & Table 3 depicts the experimental results.

5.1 Image quality analysis:

To assess the robustness and imperceptible quality of the images after it has faced some attacks, it is required to use some image quality analysis tool and parameters to quantify the similarity and distortions between the original and attacked images.

5.1.1 Peak Signal to Noise Ratio (PSNR):

The PSNR is used to indicate the degree of transparency and performance analysis of watermarking system.

$$\text{MSE}= \frac{\sum\sum [w (i, j) - w' (i, j)]2}{M*N} \qquad \text{--------} (1)$$

The PSNR in dB value is defined as:

$$\text{PSNR}=20 \log10 (\text{Maxi} / \text{RMSE}) \qquad \text{--------} (2)$$

5.1.2 Normalized Cross correlation (NCC)

Normalized Cross Correlation (NCC) is an excellent choice for finding a given pattern in an image given a known scale and orientation.

$$\text{NCC} = \frac{\sum_i \sum_j (W - w)(W' - w')}{\sqrt{\sum\sum (W - w) 2 (W' - w') 2}} \qquad \text{---------} (3)$$

Where w and w' are the averages of W and W'

5.1.3 Normalized Hamming Distance (NHD)

Normalized Hamming distance (NHD) is the similarity measure. Normalized Hamming distance is defined as in the equation (4).

$$\text{NHD} (w, w') = \frac{1}{Nw} \sum_{i=1}^{Nw} w(i) \oplus w'(i) \text{ ---------} (4)$$

Where, w and w' are the original and extracted watermarks respectively, Nw is the length of the watermark, and $\oplus$ is the exclusive-OR operator.

5.1.4 Entropy:

Entropy is calculated by using following equation Entropy defined as follows:

$$He = - \sum_{I=0}^{G-1} P(I)(\log 2\ P(I)) \ldots\ldots\ldots..(5)$$

Where: He: entropy.G: gray value of input image (0... 255).P (I): is the probability of the occurrence of the pixel of I.

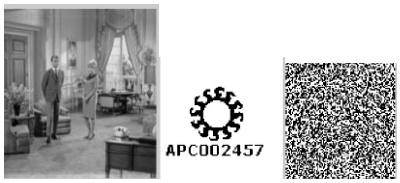


Figure 3 :(a)Original host image,(b) Original watermark and (c)encrypted watermark

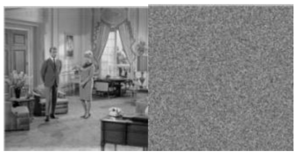


Figure 4. 0: (a) Watermarked and (b) encrypted watermarked image

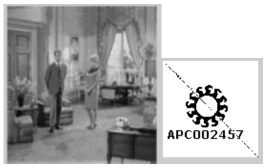


Figure 5.0(a) decrypted watermarked image and (b) Extracted watermark

Table 1
PSNR, NCC and NHDvalues

Test image	PSNR between original and watermarked images	NCC between original and extracted watermark	NHD between the original and extracted watermark
Couple	54.7518	0.9996	0.0064
Lena	54.1014	0.9995	0.0069
Girl face	52.8158	0.9996	0.0065

Table 2
Entropy analysis

Test image	Entropy of original image	Entropy of encrypted watermarked image	Entropy of original watermark logo as in Figure 3a	Entropy of encrypted watermark
Couple	7.0558	7.9463	0.4518	0.9992
Lena	7.3479	7.9490	0.4518	0.9991
Girl face	7.0428	7.9474	0.4518	0.9993
Clown	5.3684	7.9479	0.4518	0.9991
Houses	7.6548	7.9483	0.4518	0.9993

5.1.7 Histogram analysis:

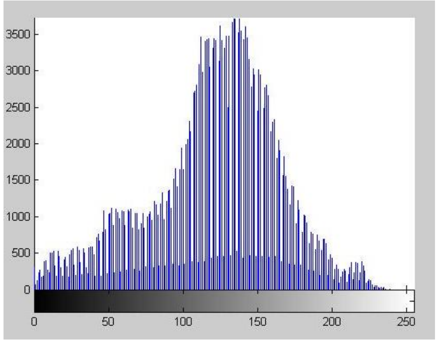


Figure 6.0 histogram of Original test image Couple image

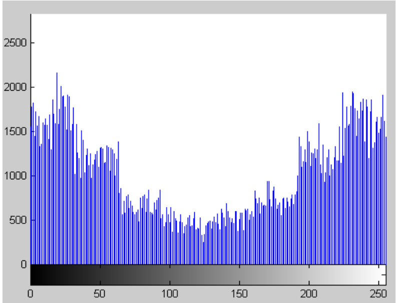


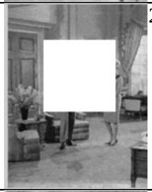
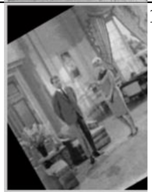
Figure 7.0 histogram of encrypted watermarked image

VI. ATTACKS AND ROBUSTNESS TESTING OF WATERMARKED IMAGE

The watermarked image in the internet environment may face intentional or accidental attack in real life situation. The normal signal processing attacks may be due to image resize, rotation, image adjustment, noise addition and filtering attack.

The watermarked image is tested with image resizing; Gaussian and salt and pepper noise addition and filtering attacks and results are quite satisfactory in extracting the watermark from the attacked watermarked and encrypted images.

Table 3
Different attacks on watermarked image and image quality parameters

Attack Type	Attacked watermarked image	PSNR btwn.host & attacked image in dB	NCC btwn W & W'	NHD btwn W & W'
No attack		54.25	0.9995	0.0063
Image cropping 200*200		23.19	0.9997	0.0074
Gaussian Noise attack (0,0.01)		18.92	0.9994	0.0055
Salt and pepper Noise attack (0.02)		20.85	0.9998	0.0055
Image rotation attack 30 degree		11.84	0.9992	0.0074
Medium Frequency		25.44	0.9994	0.0062

VII. CONCLUSIONS

In this research work we have presented a combined watermarking and encryption system which provide security of the images and as well as authenticity of the image author in the internet environment. The proposed scheme is built on DWT and SVD based image watermarking and key hash based image encryption techniques. The user specific watermarking message or logo is permanently tagged with the host image and it is in the encrypted form, if an attacker manage to get the watermark, as it is in the scrambled form , so he will not be able to get sensible information or easily replace/or distort the same. The watermarked image is encrypted before placing it for distribution to public network which will prevent unauthorized disclosure of the imagecontent and not attract the attacker easily. Thorough image quality analysis is carried out with different simulated attacks scenario. The experimental results are quite satisfactory and the system is robust against common image attacks and signal processing attacks.

REFERENCES

[1] I. J. Cox, G. Doerr, T. Furon, ”Watermarking is not Cryptography,” Proceedings of the 5th International Workshop on Digital Watermarking 2006, LNCS 4283, pp. 1-15, 2006.

[2] P. Bas, S. Katzenbeisser et al., ”First Summary Report on Hybrid Systems,” European Project IST-2002-507932, ECRYPT - Network of Excellence in Cryptology, Deliverable D.WVL.5, 2005.

[3] N. Merhav,”On Joint Coding for Watermarking and Encryption,” IEEE Transactions on Information, Theory, Vol. 52, No. 1, Jan. 2006.

[4] Chandra, D. V. S., Digital image watermarking using singular value decomposition, Proc. of the 45th Midwest Symposium on Circuits and Systems, vol.3, pp.264-267, 2002.

[5] Tapas Bandyopadhyay. Bandyopadhyay, B N Chatterji, Image Security Enhancement Through Watermarking and Cryptographic Measures, National conference : INDIACOM-2009 , New Delhi, February 2009

[6] Tapas Bandyopadhyay, Robust and secure watermarking for protecting rightful ownership, Recent Trends in Computer Technologies (RTCT) Seminar organized by B P Podder Institute of Technology and Management and CSI,28 March 2009

[7] Chang, C. C. and Y. S. Hu, Digital watermarking scheme based on singular value decomposition, Proc. of the International Symposium on Combinatorics, Algorithms, Probabilistic and Experimental Methodologies, Hangzhou, China, to appear, 2007.

[8] Chung, K. L., C. H. Shen and L. C. Chang, A novel SVD- and VQ-based image hiding scheme, Pattern Recognition Letters, vol.22, no.9, pp.1051-1058, 2001.

[9] Cox, I. J., J. Kilian, F. T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, vol.6, no.12, pp.1673-1687, 1997.

[10] Tapas Bandyopadhyay, B. Bandyopadhyay, B N Chatterji ” Attacks on Digital Watermarked Images in the Internet Environment and Their Counter Measures” International Journal of Advanced research in computer science, ISSN No. 09765697, Volume 4, No. 4, March-April 2013, page 155-159.

[11] Tapas Bandyopadhyay, B. Bandyopadhyay, B N Chatterji” Image Security through Combined Watermarking and Encryption Techniques” International Journal of electronics and Communication (IJEC), volume 1, issue 2 July 2013 Page 1-7.