IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 3, Issue 1, August 2014)

A Dual Security Approach for Image Watermarking using AES and DWT

Anjana Joshy
Department of Computer Science and Engineering
Sree Narayana Gurukulam College of Engineering
MG University,Kerala
anjanajoshy.mj@gmail.com

Neenu Suresh, Assistant Professor
Department of Computer Science and Engineering
Sree Narayana Gurukulam College of Engineering
MG University, Kerala
neenus22@gmail.com

Abstract— **This paper proposes multimedia authentication and tamper detection scheme with the security of AES (Advanced Encryption Standard) ciphered watermarking and hash function. The algorithm embeds two watermarks in the host image for authentication and tamper detection. We first used unique identification Code (UIC) as first robust watermark which is then embedded using the 2-level discrete wavelet transform (DWT). Hash code of host image is calculated and used as secondary watermark for tamper detection. This method is blind in nature. We performed several security attacks like compression attack, noise attack and cropping attack on watermarked host image and evaluated the proposed watermarking technique to examine the system robustness. Performance is recorded on the basis of PSNR and SSIM values.**

Keywords—**AES, PSNR, SSIM, UIC, Tamper Detection, Hash function.**

I. INTRODUCTION

Digital media offer a few different preferences over analog media, for example, simple editing, high quality, superior and simple duplication. High spreading of broadband systems and new advancements in advanced innovation has made possession insurance and confirmation of digital multimedia an extremely critical issue. Advanced watermarking gives a conceivable answer for the issue of simple editing and duplication of digital images, since it makes conceivable to distinguish the creator of an image by installing secret data in it.

Digital data is simple with disperse, copy and adjust which prompts the requirement for copyright insurance strategies. Digital watermarking method is one of the answers for keep away from unapproved replicating or altering of digital media information. As of late numerous watermarking techniques have been proposed to address this issue. The term 'Digital Watermarking' is characterized as the methodology of concealing a bit of computerized information in the spread information which is to be ensured and concentrated later for proprietorship confirmation [1]. A percentage of the paramount applications of watermarking system are broadcast monitoring, copyright assurance, finger printing, and ownership verification. The features of watermarking incorporate power and detectable quality. Robustness demonstrates the resistivity of watermark against distinctive sorts of attacks, for example, rotating, cropping, low pass filtering, resizing, scaling, JPEG compression, addition of noise, sharpness, contrast adjustment and histogram equalization. Those attacks are either deliberate or unintentional. Robustness is the property which is paramount for ownership confirmation although the delicacy is critical for image verification.

Robustness of watermarking scheme is acquired to a greatest level when data is stowed away in robust segments of cover data. The expanding detectable quality will additionally diminish the nature of watermarked image. The watermarking techniques are comprehensively classifications into two fundamental domains i.e. spatial domain and the transform domain. In spatial domain watermarking the watermark is implanted by straightforwardly changing the intensity values of the cover image. The most well-known system is the least significant bit (LSB) method. In transform domain the watermark is installed by adjusting the frequency coefficients of the transformed image.

The normal strategies in the transform domain are discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), and so on. As of late, singular value decomposition (SVD) was investigated for watermarking. It is a standout amongst the most valuable numerical investigation strategies having property that the singular values (SVs) of an image don not change essentially when a little perturbation is added to the image [2-5].

It is well realized that there are three fundamental commonly clashing properties of data hiding methods: indefectibility, capacity and robustness

IJDACR

[6]. It might be normal that there is no a solitary watermarking technique with the best quality as in three specified above properties have the most extreme worth without a moment's delay. Yet in the meantime it is clear that one can arrive at truly adequate quality by method for joining different watermarking schemes and by method for controls in the most ideal way operations both in the spatial and in frequency domains of an image. In paper [7] a methodology to consolidating of DWT and DCT to enhance the execution of the watermarking algorithms, which are built singularly in light of the DWT, is proposed. Watermarking was carried out by implanting the watermark in the first and second level DWT sub-bands of the host image, emulated by the application of DCT on the selected DWT sub bands. The blend of these two transforms enhanced the watermarking execution significantly when contrasted with the DWT-just watermarking methodology. Accordingly, this methodology is in the meantime, safe against copy attack. Also, the delicate data is embedded in a manner which saves robustness and dependability of the powerful part.

Robustness is the property which is essential for ownership verification as the delicacy is paramount for image verification. Robustness of watermarking scheme is acquired to a greatest level when data is covered up in powerful segments of cover data. The expanding detectable quality will likewise diminish the nature of watermarked picture. By and large data could be stowed away, straightforwardly by altering the intensity value or pixel estimation of a picture or its frequency segments [8]. The previous strategy is called spatial domain method and later is called frequency domain method. To acquire frequency components of an image, it needs to be converted utilizing any of the conversion procedures, for example, Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT), Discrete short Fourier change (DSFT)[91 10], Walsh Hadamard change (DHT) [11, 12], and Discrete wavelet Transformation (DWT)[13, 14, 15 and 16].In Transform domain casting of watermark is possible in full frequency band of an image or in specific frequency band, for example, in low frequency band or in high frequency band or in middle frequency band.

II. PROPOSED METHODOLOGY

Robust watermark and fragile watermark are the two parts of the proposed technique. Robust watermark uses the discrete wavelet transform to embed the watermark in the grey host image. The 1-level Discrete wavelet transform decomposes an image into a lower resolution approximation image (LL1) as well as horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components as shown in Fig 1 [17]:

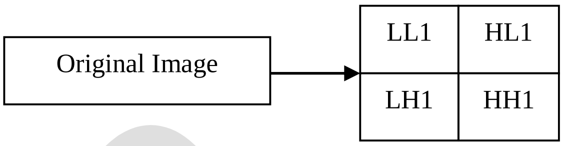


Figure 1: 1-Level Decomposition of Image

To compute 2 levels of 2D-DWT the DWT algorithm is again applied on the LL1 which further decompose the LL1 part in four sub-bands LL2, HL2, LH2 and HH2. As high frequency component is not resistant to JPEG compression so low frequency component are used for watermarked embedding. The hash code of the host grey image is being calculated and it will be used as a fragile watermark for tamper detection [18]. Fig 2 Shows the 2D-DWT process which we had used for selection of band [19].

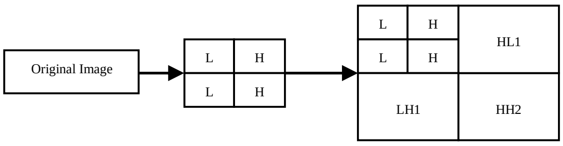


Figure 2: Second Level Decomposition of Image

Watermarking Technique

The UIC (mobile number) is the robust watermark. The UIC is the decimal number which is encrypted using the AES algorithm. Each decimal number is converted into 4 bit using the binary coded decimal (BCD) code. AES provide efficient way to encrypt the BCD code.

Fig 3 represents the entire watermark embedding process.

IJDACR

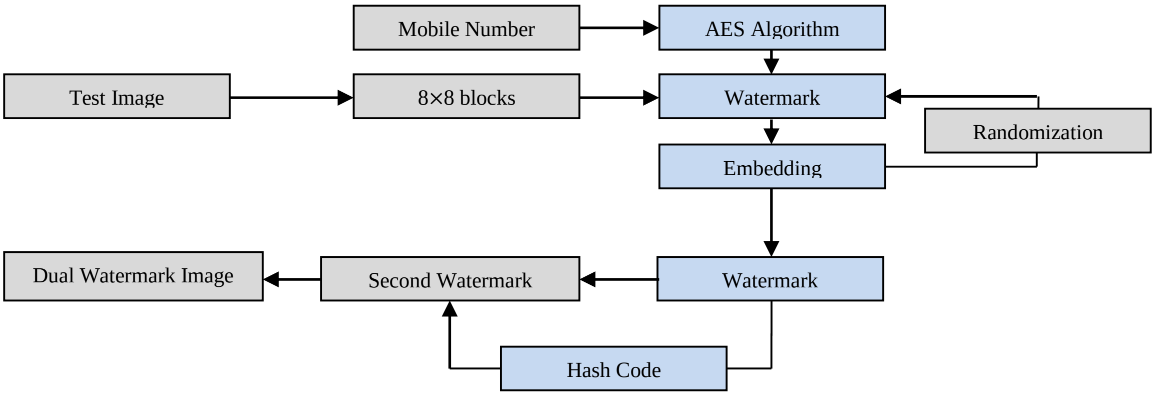


Figure 3: The Embedding of Dual Watermarks in the Host Image

Suppose the pixel of the host image is represented by f (i, j) and the binary watermark pixel by w (i, j)

$$F_k(u,v) = DWT\{fk(i,j)\}$$

If $w(i,j) = 1$ then

$$F(x,y) = \begin{cases} \Delta Q_e\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{cases} \quad (1)$$

If $w(i,j) = 0$ then

$$F(x,y) = \begin{cases} \Delta Q_o\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{cases} \quad (2)$$

Quantization to the nearest odd integer is represented by Q_o and Quantization for even number by$Q_e$in equation 1 and 2 respectively. Δ is the scaling factor and it is used to quantize either odd or even numbers. Repetition of the process is carried out until all the8×8blocks is converted into the special domain. In the second part of the technique, the fragile watermark is embedded into the host image. If the image is 512×512 then the hash code of 511×512 is calculated and the hash code is converted into the binary code to embed it into the least significant bit of first row of the image [20].

Extraction of Image

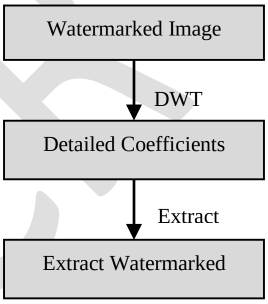


Figure 4: Flow Diagram for Watermark Extraction from Image

First of all the hash code of the image is extracted from the first row of the image. Then hash code is calculated for the image, if there is any difference between the hash codes then host image has been modified or manipulated, if not then host image is genuine.

In the Second part of Extraction process, the robust watermark has been extracted from host image [20]. In this process firstly 2-level DWT is applied to watermarked image. The watermarked image is divided into 8×8 blocks. After conversion into the DWT, the Frequency coefficients are calculated to obtain the watermark bits. The extraction of the watermark is done as shown in figure 4.

The computational formula for extraction is:

$$if\ Q\left(\frac{F_{k(x,y)}}{\Delta}\right)\ is\ odd\ then\ w(i,j) = 0$$
$$if\ Q\left(\frac{F_{k(x,y)}}{\Delta}\right)\ is\ even\ then\ w(i,j) = 1 \quad (3)$$

The watermark bit extracted is in the encrypted pattern. To obtain the original UIC reverse advanced Encryption standard (RAES) algorithm is applied on the extracted bits. There is no need for the original image as the scheme is blind in nature.

IJDACR

Fig 5 and Fig 6 describe the extraction process in two phases. In phase-1 the hash code is extracted to check whether the image is genuine or tampered and in phase 2 robust watermarks are extracted to check authentication of the image.

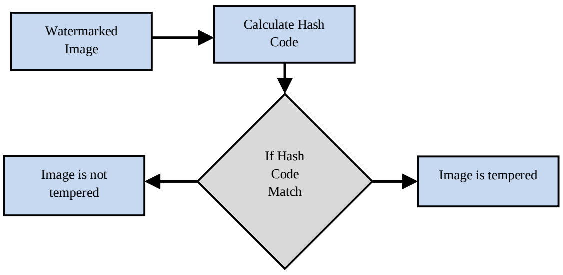


Figure 5: From Host Image Extraction of Hash Code is generated

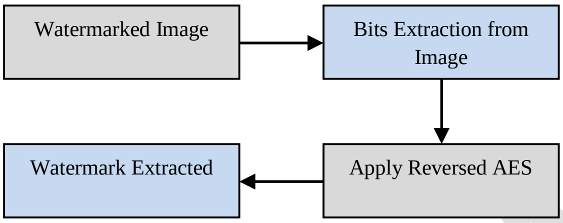


Figure 6: Extraction of Robust Watermark from Image

III. Simulation & Results

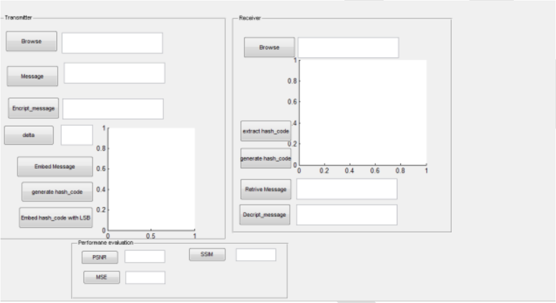
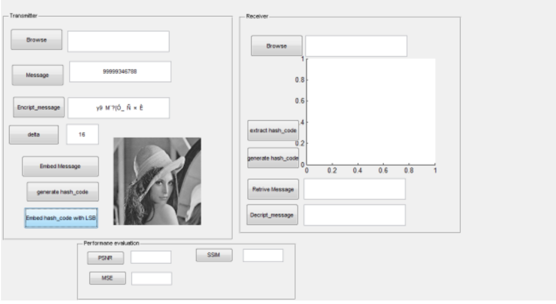
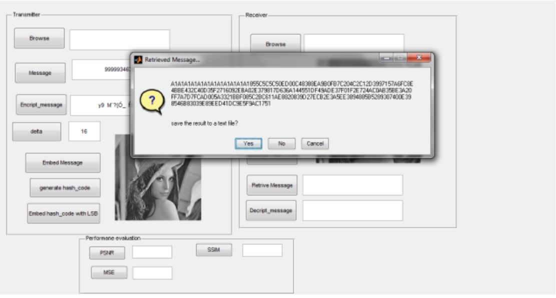


Figure 7: Graphical User Interface Design for Digital Watermarking



Message: 99999346788
Encript_message: y9 M˜?|Ó_ Ñ × Ê
delta: 16

Figure8: Encryption Step for Cover Image

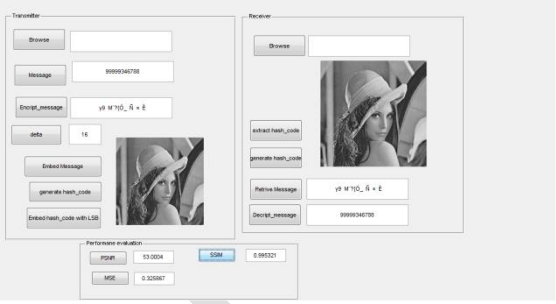


Retrieved Message...

A1A1A1A1A1A1A1A1A1A1A1A1A1855C5C5C50ED00C48388EA980FB7C204C2C12D3997157A6FC8E
4B8E432C40D35F2716092EBA02E379817D636A144551DF49ADE37F01F2E724AC0AB35BE3A20
FF7A7D7FCAD005A332188F085C28C611AE8820839D27ECB2E3A5EE3894885B5289307400E39
8546B83039E89EED41DC9E5F9AC1751

save the result to a text file?

Figure9: Hash Code Generation on Watermarked Image



Message: 99999346788
Encript_message: y9 M˜?|Ó_ Ñ × Ê
delta: 16
Retrive Message: y9 M˜?|Ó_ Ñ × Ê
Decript_message: 99999346788
PSNR: 53.0004
MSE: 0.325867
SSIM: 0.995321

Figure10: Recovery of Text Data from Watermarked Image

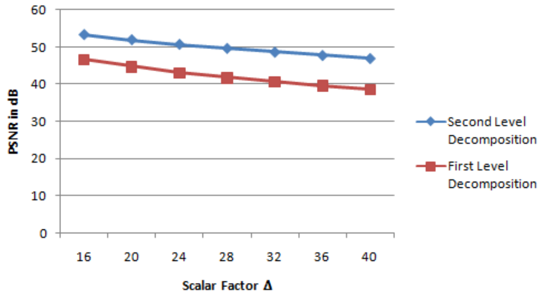


Figure 11: Comparison between PSNR with respect to Δ

Table 1: SSIM values for different values of Δ

Values of Δ	SSIM for different images		
	Lena	Pepper	Airplane
Δ=16	0.9956	0.9941	0.9821
Δ=20	0.9944	0.9920	0.9745
Δ=24	0.9933	0.9905	0.9652
Δ=28	0.9923	0.9880	0.9632
Δ=32	0.9813	0.9820	0.9611
Δ=36	0.9705	0.9778	0.9520
Δ=40	0.9698	0.9705	0.9456

Table 2: PSNR values for different values of Δ

Values of Δ	PSNR for different images		
	Lena	Pepper	Airplane
Δ=16	53.3377	50.2256	48.5621
Δ=20	51.9442	49.2612	47.3642
Δ=24	50.6956	48.2563	46.8295
Δ=28	49.5991	46.9589	45.1271

Δ=32	48.5695	44.5378	44.3214
Δ=36	47.6862	43.1229	42.9895
Δ=40	46.8601	41.5621	41.2362

Table 3: PSNR values for single level decomposition at different values of Δ

Values of Δ	PSNR for Lena image
Δ=16	45.8854
Δ=20	44.2011
Δ=24	42.9512
Δ=28	41.6702
Δ=32	40.0211
Δ=36	39.5012
Δ=40	37.3012

Table 4: Performance of robust algorithm to attacks

Type and Strength of Attacks	Performance
JPEG Compression 25%	Extracted Successfully
JPEG Compression 50%	Extracted Successfully
JPEG Compression 75%	Extracted Successfully
25% vertical Cropping	Extracted Successfully
50% vertical Cropping	Extracted Successfully
75% vertical Cropping	Extracted Successfully

Table 5: Calculation of hash code for tamper detection

Airplane image with original hash code	Hash code after Tampering of Airplane Image	Edited Part of Airplane Image
FF7A7D7FCAD005A3321BB	F085C2BC611AE8820839D	Tail Edited
FF7A7D7FCAD005A3321BB	27ECB2E3A5EE3894885B5	Wing Edited
FF7A7D7FCAD005A3321BB	46B83039E89EED41DC9E5	Tip Edited

IV. CONCLUSION

This paper shows an image watermarking technique based on a 2-level discrete wavelet transform. This technique can embed the invisible robust and fragile watermarks which are useful for copyright protection and content authentication and tamper detection. PSNR achieved by our method is higher than 45 dB and SSIM value is greater than 0.99. We obtained satisfying results and showed that the technique can resist different various compressions filtering and many other attacks.

REFERENCES

[1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," in Proc. of the IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

[2] R. Sun, H. Sun, and T. Yao, "A SVD and quantization based semifragilewatermarking technique for image authentication," in Proc.Int. Conf. Signal Process., pp. 1592–1595, (2002)

[3] C. C. Chang, P. Y. Tsai, and M. H. Lin, "SVD-based digital image watermarking scheme," Pattern Recogn. Lett. 26, 1577–1586, (2005).

[4] J. M. Shieh, D. C. Lou, and M. C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition," Comput. Stand. Inter. 28, 428–440, (2006).

[5] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia 4, 121–128, (2002).

[6] Chih-Chin Lai and Cheng-Chih Tsai.(November 2010) 'Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition', IEEE Transactions On Instrumentation And Measurement Vol.59, No.11, pp. 3060-3063.

[7] Chun-Shien Lu and Hong-Yuan Mark Liao.(October 2001) 'Multipurpose Watermarking for Image Authentication and Protection' IEEE Transactions On Image Processing Vol. 10, No.10, pp.1579- 1592.

[8] V. Potdar, et al "A Survey of Digital Image Watermarking Techniques", in Proc.of the EEE International Conference on Industrial Informatics, Australia Perth, pp. 709-716, 2005.

[9] Liu Quan, AI Qingsong "A combination of DCT based and SVD based watermarking, ICSP proceedings of IEEE International conference on signal processing, pp. 873-876, 2004.

[10] Feng Liu, et al. "A Watermarking Algorithm for Digital Image Based on DCT and SVD" Congress on Image and Signal Processing, 2008.

[11] Emad E. Abdallah, et al. "A robust block-based image watermarking scheme using fast Hadamard transform and singular value decomposition" proceedings of The 18th International Conference on Pattern Recognition, pp:673 - 676 , 2006.

[12] Tang Xianghong, Yang Lianjie, YueHengli, Yin Zhongke, "A Watermarking Algorithm Based on the SVD and HadamardTransform", Proceedings of International Conference on Communications, Circuits and Systems,Volume 2, pp. 874-877 , 27-30 May 2005.

[13] Ali Al-Haj, "A Hybrid Digital Image Watermarking Algorithm", 4thInternational Conference on Innovations in Information Technology. pp: 690 - 694 Nov. 2007.

[14] Liu Liang and Sun Qi "A new SVD-DWT composite watermarking", ICSP proceedings of IEEE International conference on signal processing .2006

[15] Jung-Chun Liu, Chu-Hsing Lin, and Li-ChingKuo" A Robust full band image watermarking scheme" Proceedings on IEEE .2006

[16] Qiang Li, et al, "Adaptive DWT-SVD Domain Image Watermarking Using Human Visual Model" proceedings of 9thinternational conference on advanced communication Technology, Volume 3, pp: 1947 - 1951, Feb.2007.

[17] N. Kashyap, and G. Sinha, "Image Watermarking Using 2-Level DWT", Advances in Computational Research, ISSN: 0975 -3273 & E- ISSN: 0975-9085, Vol. 4, Issue 1,pp.-42-45, 2012,

[18] A. G. Konheim, "Hashing in Computer Science: Fifty Years of Slicing and Dicing", John Wiley & Sons, Inc, 2010.

[19] I. R. Farah, I. B. Ismail, and M. B. Ahmed, "A Watermarking System Using the Wavelet Technique for Satellite Images." International Journal of Engineering and Applied Sciences, pp. 197-201, 2007.

[20] Jassim, Jassim, Taha, RaedAbd-Alhameed, and Hussain Al Ahmad. "A new robust and fragile watermarking scheme for images captured by mobile phone cameras." In Communications, Signal Processing, and their Applications (ICCSPA), 2013 1st International Conference on, pp. 1-5. IEEE, 2013.