MULTIMEDIA DATA SECURITY THROUGH A NOVEL APPROACH BY USING VISUAL CRYPTOGRAGHY & DIGITAL WATERMARKING

Miss Manisha A. Wherate
P.G Department of CS & Engg,
SGB Amravati University
wheratemanisha33@gmail.com

Dr. S. S. Sherekar
P.G Department of CS & Engg,
SGB Amravati University
ss_sherekar@rediffmail.com

Dr. V. M. Thakare
P.G Department of CS & Engg,
SGB Amravati University
vilthakare@yahoo.co.in

Abstract:

Data security in Multimedia is most significant concern for the networking technology because of the ease of the duplication, manipulation and also distribution of the multimedia data. The digital watermarking is technique for information hiding which hide the decisive information in the original data for protection illegal duplication and distribution of multimedia digital data. This paper proposed a novel frame work consist of the DCT & DWT based image watermarking methods. Results are tested by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE). The analytical results demonstrate that the watermarks generated with the proposed algorithm are invisible and the quality of recovered image and the watermarked image are improved.

Introduction:

With the widespread distribution of digital information over the internet, the protection of intellectual property rights has become increasingly important. These information, which include still video, images, audio, or text are stored and transmitted into digital format. Information stored in form of digital format can be easily copied without loss of quality and efficiently distributed [1]. This digital watermarking is then introduced and used to solve this problem. Digital watermarking technique is a branch of information hiding which is mostly used to hide proprietary information in digital media like photographs, images, digital music, or digital video [2-3]. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. The Copyrighted material can be easily exchanged or transfer over the networks, and has caused major concerns to those content providers who produce these digital contents. The digital image watermarking techniques can be classified into two major classes: Frequency Domain Watermarking (FDW) and Spatial Domain Watermarking (SDW). Compared to spatial domain techniques [4], frequency-domain watermarking techniques proved to be more effective with respect to achieving the robustness requirements of digital watermarking algorithms [5]. Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT). However, DWT has been used in digital image watermarking more frequently due to its better and excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. The performance improvements in DWT-based digital image watermarking algorithms could be obtained by increasing the level of DWT.

This paper presents the comparison between two watermarking technique that is DCT and DWT. The Performance measure is done on the basis of parameters PSNR and MSE. In the digital watermarking the secret information is hided into the original data for protecting the ownership rights of the multimedia data. The watermarking techniques may divide on the basis of domain. The spatial domain techniques directly work on the pixels and the frequency domain works on the transform coefficients of the images. This paper elaborates the most important method of transform domain and focuses the merits and demerits of these techniques.

Background:

Spatial Domain

In image processing an analogue image can be described as a continuous function over a two-dimensional surface. The value of this function at a specific coordinate on the lattice specifies the luminance or brightness of the image at that location. A digital image version of this analogue image contains sampled values of the function at discrete locations or pixels. These values are said to be the representation of the image in the spatial domain or often referred to as the pixel domain. The oldest and the most common used method in this category is the insertion of the watermark into the least significant bits (LSB) of pixel data [4][5]. In decimal representation the watermarked image has pixel values of 234, 223, 188 and 34. Since modification of pixel values occurs in the LSB of the data, the effect to the cover image is often visually indifferent. This effect however becomes more apparent as more bits are used to hide the watermark. The major limitations in spatial domain are the capacity of an image to hold the watermark. In the case of LSB technique, this capacity can be increased by using more bits for the watermark embedding at a cost of higher detection rate. The

capacity can also be improved by means of lossy embedding the watermark. The watermark is quantized before the embedding process. Improving this limitation seems to be one of the major drives in spatial domain research.

B. Transform Domain

Transform domain embeds a message by modifying the transform coefficients of the cover message as opposed to the pixel values. The transform domain has the effect in the spatial domain of apportioning the hidden information through different order bits in a manner that is robust. There are many numbers of transforms that can be applied to digital images, but there are notably three most commonly used in image watermarking. They are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

Discrete Cosine Transform

DCT is related to DFT in a sense that it transforms a time domain signal into its frequency components. The DCT however only uses the real parts of the DFT coefficients. In terms of property, the DCT has a strong "energy compaction" property and most of the signal information tends to be concentrated in a few low-frequency components of the DCT. The JPEG compression technique utilizes this property to separate and remove insignificant high frequency components in images.

Discrete Wavelet Transform

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. A wavelet series is a representation of a square-integrable function by a certain orthonormal series generated by a wavelet. Furthermore, the properties of wavelet could decompose original signal into wavelet transform coefficients which contains the position information. The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients. Watermarking in the wavelet transform domain is generally a problem of embedding watermark in the subbands of the cover image. There are four subbands created at the end of each level of image wavelet transformation: they are Low-Low pass subband (LL), High-Low (horizontal) subband (HL), Low-High (vertical) subband (LH) and High-High (diagonal) pass subband (HH). Subsequent level of wavelet transformation is applied to the LL subband of the previous one.

Related work:

In previous workdone most of the authors works on different technique of watermarking such as LSB that is spatial domain based and DCT, DWT which are transform domain based. Many digital watermarking methods have been proposed for various applications [1] Several studies focus quantization index modulation (QIM) and spread spectrum-based watermarking is still also attractive[2] for tolerance. From the perspective of the image-quality of watermarked images, image-adaptive watermarking and informed embedding that utilizes the characteristics of the target image are effective in improving the imperceptibility of watermarks. To contribute to the objective image-quality of watermarked images, image-quality guaranteed watermarking (IQGW) methods that generate watermarked images of a desired image-quality independent of the characteristics of the target images and without trial and error, have been proposed On the other hand, a modulo arithmetic-based watermarking method for JPEG-coded images has also been proposed [3]. The method offers the user the flexibility of choosing the coefficients for watermarking in each 8×8-sized quantized discrete cosine transformed (DCT) matrix, and extracts hidden data using neither reference images nor the knowledge of the position of chosen coefficients. Furthermore, because of the use of modulo arithmetic- based modulation of data, it is capable of reducing the distortion caused by watermarking. However it is only for JPEG-coded images and its image-quality performance has not been analyzed enough yet. This LSB insertion is very vulnerable to a lot of transformations, even the most harmless and usual ones. Lossy compression, e.g. JPEG, is very likely to destroy it completely. Any other kind of picture transformation, like blurring or other effects, usually will destroy the hidden data.

Analysis of Existing methodology:

In [5] authors proposed such hybrid approach that uses the visual cryptography and watermarking technique together. In this proposed scheme, first the secret image is breaks into shares using (2, 2) VC scheme and then hides the shares using Digital watermarking inside some cover images. To embed the secret share into cover images, discrete cosine transformation (DCT) technique is used that change the image into frequency domain.

In the proposed scheme [6], initially the secret data is encrypted using visual cryptography and then cipher image is embedded into another carrier images using steganography. The mechanism is a one compact form of both the data security techniques. For encryption process, the secret image is decomposed into its CMY components and the Random grids of the individual components are generated. These new grids are then embedded inside carrier image by using a steganographic algorithm in the spatial domain with LSB replacement based on DCT coefficients of the pixels.

In [7], another novel technique was invented for robust wavelet-based watermarking. The main idea of this paper embeds the signature data to the selected group of wavelet transform coefficients, varying the watermark strength according to the subband level and the group where the corresponding coefficients reside. Initially, the input image decompose into 4 levels by DWT, so we get approximation subbands with low frequency component and 12 detail

subbands with high frequency component. Next, the author detect edge in each component by using Sobel edge detector, so it is forming 2 groups of coefficients, at the meanwhile, morphological dilation capture the coefficients that near the edge for forming another group. In the end, the watermark energy distributes between these groups with a variable strength. The results of all the discussed methods and schemes in above papers are successfully executed. The main security problems are overcome in the experimental results of visual cryptography process. In [9] the scheme uses a color index table to hide and recover the image. In recovering a secret image, small memory space and simple computations are required.

Proposed methodology:

In this proposed scheme two watermarking technique is applying on two shares which is created by secrete share visual cryptography. Block diagram shows the actual working of proposed scheme shown in figure 1

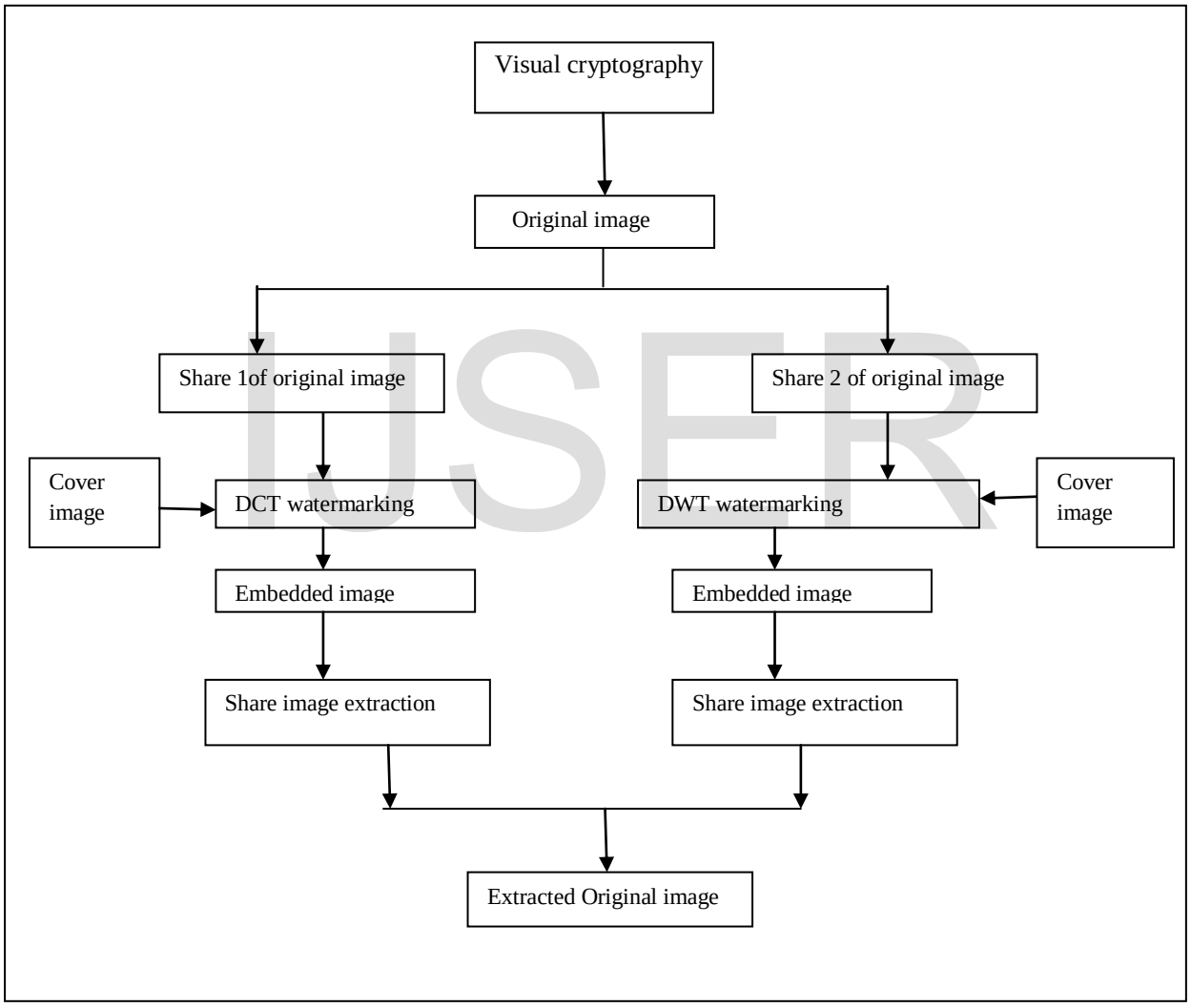

Figure 1: block diagram proposed framework

The main steps which used in DCT:

1) Segment the image into non-overlapping blocks of size 8x8.

2) Next Apply forward DCT to each of these blocks.

3) Now apply some block selection criteria.

4) Apply coefficient selection criteria (e.g. highest).

5) Next, Embedded watermark by modifying the selected Co-efficient.

6) Apply inverse DCT transform on each block.

The most common DCT definition of a 1-D sequence of length N is:

$$c(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (1)$$

For u=0, 1, 2, 3...., N-1.Similarly, the inverse transformation for 1-D sequence of length N is

$$f(x) = \sum_{u=0}^{N-1} \alpha(u)c(u) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (2)$$

For both the equations α (u) is defined as

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}}, & u = 0 \\ \sqrt{\frac{2}{N}}, & u \neq 0 \end{cases} \quad (3)$$

In DCT the first transform coefficient is DC coefficient and all others are AC coefficients. The 2-D DCT transform is extension of 1-D DCT and is given by:

$$c(u,v) = \alpha(v)\alpha(u) \sum_{x,y=0}^{N-1} \sum f(x,y) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (4)$$

For u, v=0, 1, 2, 3....., N-1 and α (u) and α (v) defined in equation (3). The 2-D DCT inverse transforms is given by:

$$f(x,y) = \sum_{u,v=0}^{N-1} \sum \alpha(v)\alpha(u)c(u,v) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (5)$$

Discrete Wavelet Transform:

DWT of the image produces multi resolution representation of an image. This multi resolution representation provides a simple framework for the image to interpret information. DWT divides the image into low frequency quadrants and high frequency quadrants. The low frequency quadrant is again split into two more parts of low and high frequencies and this process is repeated until the signal has been entirely decomposed.

The DWT is applied on the host image to decompose the actual image into four non overlapping multi resolution coefficient sets, and the coefficients are:

$$W_{LL}^{J} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} g(x)g(y)W_{LL}^{J-1}(2u-x)(2v-y) \quad (6)$$

$$W_{LH}^{J} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} g(x)h(y)W_{LL}^{J-1}(2u-x)(2v-y) \quad (7)$$

$$W_{HL}^{J} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} h(x)g(y)W_{LL}^{J-1}(2u-x)(2v-y) \quad (8)$$

$$W_{HH}^{J} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} h(x)h(y)W_{LL}^{J-1}(2u-x)(2v-y) \quad (9)$$

Where J is the level of the 2-D DWT, h (n) and g (n) are the impulse response. Figure 6 shows the schematic diagram of 2D wavelet transform. By using this figure we can analyze in which way the 2D wavelet transform are performed.

Possible outcome and result:

The possible results may give the actual layering of these two technologies that is visual cryptography and watermarking technique. The performance estimation is on the basis of different parameter like PSNR and MSE values calculated from watermarked image. In this paper two techniques are compared and quality of image is calculated by analyzing the values of PSNR.

As the performance measure we calculate the difference between the watermark signals in both the original watermarked image and the reconstructed watermarked image by applying DCT and DWT. The difference value is further converted to Peak-to-Signal Ratio (PSNR) to give a more representative picture of distortion severity relative to signal strength. The PSNR is calculated by PSNR = 20log10 (255/RMSE), where RMSE is the square root of Mean Squared Error between the original and recovered watermark signal. All watermarked image extracted completely after adding noise, most of watermark is recovered, but in other watermarking technique that is LSB, watermark recovered image is totally distorted. Compare with PSNR in different specific algorithm, LSB contains lowest PSNR, both DCT and DWT has their strong point. In other words, the robustness of DCT and DWT in frequency domain are far better than LSB in spatial domain, both DCT and DWT have their advantages each. One major reason why transform domain is more robust than spatial domain because of watermark embeds into the band of the transformed host image. Watermarking in high frequency band tends to be less robust but has a lesser effect on the quality of original image, while watermarking in low band will achieve a better robustness but at the expense of significant alteration to the original image.

Acknowledgement:

I would like to thank my guide Dr. S. S. Sherekar, dept. of computer science and Engg., SGB Amravati university. I would like to give special thanks to our research center head, Dr. V. M. Thakare, SGB Amravati University. I would like to mention the special thanks to AICTE for providing the funds under RPS, under which I am able to carry out my research work.

Conclusion:

Digital watermarking is very useful method for providing security to the digital media on the internet technology. In this paper, comparisons and performance measures is done on the basis of two parameters PSNR and MSE watermarking technique (DCT, DWT). The analytical result shows the different effective algorithms of watermark. The result indicates frequency domain is more robustness than spatial domain.

Digital watermarking is still a challenging research field area with many interesting problems, such as it does not prevent distribution or any copying and also cannot survive in every possible attack. The future research pointer is the development of transparent, secure and truly robust watermarking technique for different digital media including video, audio and images.

References:

[1] C. C. Chang, C. C. Lin, T. H. N. Le, and H. B. Le, "Self-verifying visual Secret sharing using error diffusion and interpolation techniques," IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 790–801, Dec. 2009.

[2] Fouad M., El Saddik, A., Jiying Zhao Petriu, E., "Combining cryptography and watermarking to secure revocable iris templates", Instrumentation and Measurement Technology Conference (I2MTC), IEEE, vol., no., pp.1, 4, 10-12 May 2011

[3] Pereira, S., Pun, T.: Robust Template Matching for Affine Resistant Image Watermarks, *IEEE Transactions on Image Processing*, vol.9, 1123-1129, 2010.

[4] Jessica Fridrich and Jan Kodovsky, Rich Models for Steganalysis of Digital Images, IEEE Transaction on Information Forensics and Security, Vol. 7, No. 3, pp. 868-882, June 2012.

[5] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," IEEE Trans. Inform. Forensics Security, vol. 6, no. 3, pp. 920–935, Jun. 2010.

[6]Yongsheng Liu, Jie Li, and Mohsen Guizani, "PKC Based Broadcast Authentication using Signature Amortization for WSNs", IEEE Transactions on wireless communications, vol. 11, no. 6, 2106-2115, June 2012.

[7] Naskar P., Chaudhuri A, Chaudhuri Atal, Image Secret Sharing using a Novel Secret Sharing Technique with Steganography, IEEE CASCOM, Jadavpur University,2010, pp 62-65.

[8] Olaniyi, O.M, O.T Arulogun, E.O. Omidiora, & Okediran O.O, "Performance Evaluation of modified Stegano-Cryptographic model for Secured E-Voting", 2014, International Journal of Multidisciplinary in Cryptology and Information Security(IJMCIS),Vol.3 No.1, pp 1 -8.

[9] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications". IEEE Journal on Selected Areas in Communications, Vol.16, No.4, pp. 573–586 may 2012.

[10] D. Goya, R. Terada., "Java Cryptographic Library for Smartphone", Journal Latin America Transactions IEEE, Vol.10, 2012, pp.1377-1384.