ISSN No:-2456-2165

An Efficient Algorithm for Image Steganography or Visible Watermarking

Rafidison Maminiaina Alphonse
Telecommunication Automatic Signal Image Research Laboratory/Doctoral School in Science and Technology of Engineering and Innovation/ University of Antananarivo
Antananarivo 101, Madagascar

Ramafiarisona Hajasoa Malalatiana
Telecommunication Automatic Signal Image Research Laboratory/Doctoral School in Science and Technology of Engineering and Innovation/ University of Antananarivo
Antananarivo 101, Madagascar

Randriamitantsoa Paul August
Institution: Telecommunication Automatic Signal Image Research Laboratory/Doctoral School in Science and Technology of Engineering and Innovation/ University of Antananarivo Antananarivo 101, Madagascar

Abstract:- Commonly, a specific algorithm is dedicated for image steganography and one else for watermarking. This publication is a presentation of one method which can manage both. Watermark or secret image is binary image as default and the medium can be an image color or gray level with size greater than the first one. Singular Value Decomposition (SVD) and Discrete wavelet transform (DWT) are the mathematic approach used. They are popular on these domains but the way to operate is different for each algorithm. An insertion of new two parameters is the particularity of our method, in which we decide if we process with steganography or watermarking. Note that we are talking here about visible.

Keywords:- *Steganography; Visible Watermarking; Discret Wavelet Transform; Singular Value Decomposition.*

I. INTRODUCTION

Two persons wants to share an important secret information however another person is present to supervise the communication between both. These people are looking for a solution to cover up the information by adding it in medium to avoid any suspicion. This kind of art and science of invisible communication is called “Steganography”. This word is come from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images [1][5].

Watermarking is art of protecting an information with signature. It may be visible or invisible. Steganography differs from watermarking in the sense that where watermarking focuses to protect the medium image with watermark image depending on medium owner. Medium image is important for watermarking however it is not the case for steganography in which the secret message is important and nobody suspects the presence of hidden information.

To ensure a good understanding of this algorithm, we develop into the first paragraph the notion of Discrete Wavelet Transform (DWT) then Singular Value Decomposition (SVD) followed by the related work, testing, results and conclusion.

II. PRELIMINARIES

A. Discrete Wavelet Transform

DWT is a multilevel transformation method. After applying this transformation, the image is decomposed into four wavelet sub bands as shown in Fig. 1. We describe in following the different type of wavelet sub bands: LL-approximate, HL-horizontal, LH- vertical, and HH-diagonal. LL position isin top-left side of the wavelet sub band which has a low frequency. It obtained through Low Pass Filtering (LPF) in both row and column directions. This sub band is the most significant part of the image which contains approximate value of an image. LL has highest robustness level among all wavelet sub bands, it able to maintains information therein (Abu et al. 2014) (Adi et al. 2015).

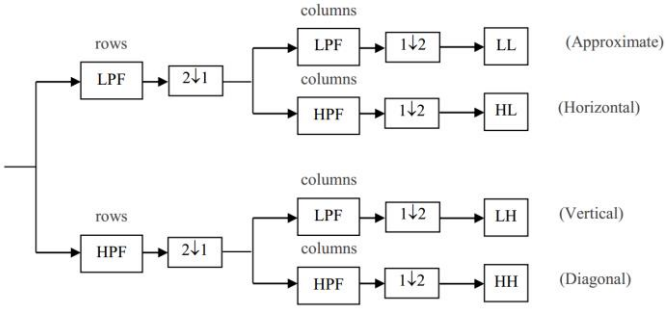


Fig. 1. Decomposition scheme DWT Level on an image

Fig. 2. Illustration of DWT transform

The subdivision of image in top-right part is the horizontal detail of the image called HL. It is generated from LPF in row order followed by High Pass Filtering (HPF) in

column order. Conversely, LH is resulted from process of HPF in row order and LPF in column order. It depicts vertical element of the image and located at the bottom-left side of wavelet sub band. The last part of wavelet sub band is HH, which is the diagonal feature of the image. This sub band contains high wavelet coefficient, hence HH is vulnerable to attacks. DWT is able to decompose an image into multilevel wavelet sub bands as shown in Fig.2. The next level of decomposition is generally performed in LL to get the higher level of wavelet sub band (LL2, HL2, LH2, and HH2) and so on. The highest level of wavelet decomposition is when it reaches a single coefficient value.

B. Singular Value Decomposition

SVD is a mathematical operation to change X matrix form to$U$, $S$and Vmatrix. The singular values of the matrix X is the composition of the diagonal matrix$S$. Whereas, the orthogonal matrices U and$V$ contains the left and right singular values of matrix X respectively.

$$SVD(X) \quad [U\ S\ V] = \quad (1)$$

$$X = U * S * V^T \quad (2)$$

where,$S$is a diagonal matrix with large singular value contains in its diagonal entries.V^T is a conjugate transpose of matrix$V$. $U$and V are complex or real unitary matrices, such that $U * U^T$ and $V * V^T$will result in identity matrix [2][4][5].

III. RELATED WORK

A. Embedding algorithm

- Step 1: Convert watermark or secret image to binary image $M(l_M \times c_M)$ size $l_M \times c_M$.
- Step 2: Decompose the medium image to RGB if it is an image color and consider only blue matrix. For gray level image, no operation is required. We note I $(l_I \times c_I)$ the result.
- Step 3: Reshape M to vector $M_R(1, l_M \times c_M)$
- Step 4: Decompose I to many block $B_{k=1,2,\ldots,(l_M \times c_M)}$. The size of each block is $(l_I/l_M) \times (c_I/c_M)$
- Step 5: Apply DWT to each B_k

$$(LL_k, HL_k, LH_k, HH_k) = DWT(B_k) \quad (3)$$

- Step 6: Apply SVD to each approximate matrix LL_k

$$(U_k, S_k, V_k) = SVD(LL_k) \quad (4)$$

- Step 7: Insert M_R

If $M_R(x) = 1$ where x indicates the row

Consider a diagonal matrix A_w same size as S_k and a parameter reference α

$$A_w = \begin{bmatrix} a_{max} & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & a_{min} \end{bmatrix} \quad (5)$$

$$S_{wk} = S_k + \alpha A_w \quad (6)$$

$$LL_{wk} = U_k * S_{wk} * V_k^T \quad (7)$$

$$B_{wk} = IDWT(LL_{wk}, HL_k, LH_k, HH_k) \quad (8)$$

Where S_{wk}, LL_{wk}, B_{wk} are the singular value watermarked, approximate watermarked, block watermarked. IDWT is the operation of inverse discrete wavelet transform.

If $M_R(x) = 0$, don't modify the block B_k

- Step 8: Assemble all block to form watermarked image I_w. I_w is the bleu matrix then constituting the watermarked image in case of color image.
- Step 9: A_w and α are the two reference parameters which define the type of operation steganography or watermarking. Minimum value corresponds to steganography and once you increase, it becomes a visible watermarking robust, we are able to see the mark in background. If they are maximum, we cannot recognize the medium like encrypted however the secret image can be extracted even the attack is so strong.

B. Extraction algorithm

- Step 1: Decompose I_w (blue matrix for an image color) to many block $B_{wk=1,2,\ldots,(l_M \times c_M)}$. Prefix w in matrix index means watermarked
  - Step 2: Apply DWT to each B_{wk}

$$(LL_{wk}, HL_{wk}, LH_{wk}, HH_{wk}) = DWT(B_{wk}) \quad (9)$$

  - Step 3: Apply SVD to each approximate matrix LL_{wk}

$$(U_{wk}, S_{wk}, V_{wk}) = SVD(LL_{wk}) \quad (10)$$

- Step 4: Extract M_R

Calculate A_w

$$A_w = (S_{wk} - S_k)/\alpha \quad (11)$$

Calculate the determinant of A_w

$$M_R(x) = \begin{cases} 1\ if\ \det(A_w) \geq 1 \\ 0 \quad otherwise \end{cases} \quad (12)$$

- Step 5: Reshape M_R with size $l_M \times c_M$ to obtain the watermark/secret image.

IV. TESTS AND PERFORMANCE ANALYSIS

In this paragraph, some experiments are conducted to evaluate therobustness and invisibilityof the proposed algorithm scheme. Invisibility and robustness are important for steganography and robustness is enough for watermarking because the mark is visible and used to protect the medium [3].

Fig.3. illustrates the original host images (Lena and Barbara) and the watermark image used during this test.

(a) (b) (c)

Fig. 3. Original image: (a) Lena; (b) Barbara; (c) watermark images

As we all know, the imperceptibility and robustness of the watermark is a pair of contradictions in digital watermarking schemes. To make a balance between imperceptibility and robustness, we analyze the effect of different value of α on the watermarked images and extracted watermarks. As one of the evaluation indexes of watermark imperceptibility, the structural similarity (SSIM) index is adopted to calculate the similarity between original image and its watermarked version, which is defined as:

$$SSIM = l(I, I_w)c(I, I_w)s(I, I_w) \quad (13)$$

$$l(I, I_w) = \frac{2\mu_I \mu_{I_w} + C_1}{\mu_I^2 + \mu_{I_w}^2 + C_1} \quad (14)$$

$$c(I, I_w) = \frac{2\sigma_I \sigma_{I_w} + C_2}{\sigma_I^2 + \sigma_{I_w}^2 + C_2} \quad (15)$$

$$s(I, I_w) = \frac{\sigma_{II_w} + C_3}{\sigma_I \sigma_{I_w} + C_3} \quad (16)$$

Where $l(I, I_w)$, $c(I, I_w)$, and $s(I, I_w)$ are three comparison functions for luminance, contrast, and structure, respectively; μ_I and σ_I are the average and variance of the host image I; μ_{I_w} and σ_{I_w} are the average and variance of the watermarked image I_w ; σ_{II_w} is the covariance between these two images; and C_1, C_2, and C_3 are three parameters used to keep stability. To evaluate the robustness of the proposed method, the normalized correlation coefficient (NCC) is utilized to investigate the correlation between the original watermark and the extracted watermark. For a watermark image W with a size of $N \times N$, the definition of NCC can be formulated as:

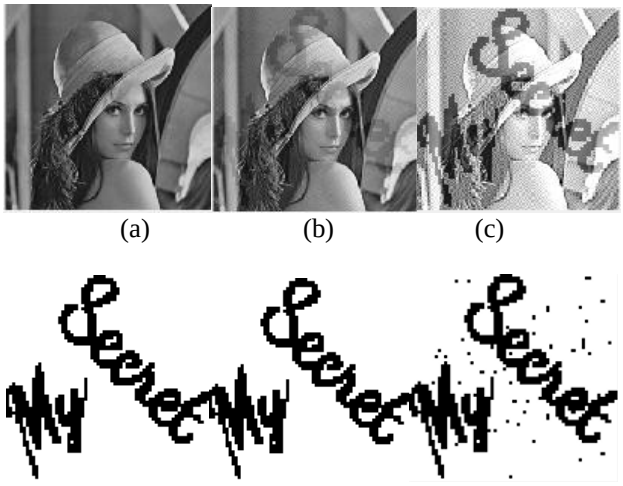
$$NCC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} [W(i,j) \times W^*(i,j)]}{\sum_{i=1}^{N} \sum_{j=1}^{N} [W(i,j)]^2} \quad (17)$$

where W^* is the extracted watermark. The normal value of SSIM and NCC is between 0 and 1. In addition, a greater value of SSIM indicates a better watermark invisibility, while a greater value of NCC implies a better robustness.

Let's add the image secret/watermark to both medium by fixing A_w and α as below:

$$A_w = \begin{bmatrix} 5 & 0 \\ 0 & 1 \end{bmatrix}, \alpha = \{5, 20, 80\} \quad (18)$$

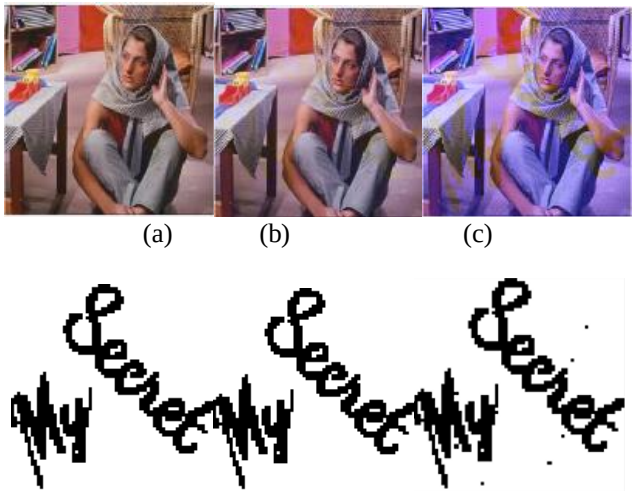
Steganography operation is favorable when α is less than 20 but once it increases, we trigger to discreet visible watermarking. If the aim is to highlight the mark, we must choose a higher value of α. In this case, there is a little noise in extracted watermark image. We illustrate these explanations with the following figures Fig.4. and Fig.5.



(a) (b) (c)

(d) (e) (f)

Fig. 4. Watermarked image of Lena : (a) $\alpha = 5$, (b) $\alpha = 20$, (c) $\alpha = 80$.Secret/watermark image: (d) extracted from (a), (e) extracted from (b), (f) extracted from (c)



(a) (b) (c)

(d) (e) (f)

Fig. 5. Watermarked image of Barbara : (a) $\alpha = 5$, (b) $\alpha = 20$, (c) $\alpha = 80$.Secret/watermark image: (d) extracted from (a), (e) extracted from (b), (f) extracted from (c)

SSIM value is important for steganography because nobody should know the presence of secret message in medium image. However, to protect a medium, SSIM value is degraded due of making evidence the mark. According to our experience, we have TABLE I which contains SSIM for medium and NCC for mark value.

TABLE I. SSIM VALUE FOR MEDIUM AND NCC VALUE FOR WATERMARK

α		5	10	20	40	80
Lena	SSIM	0.9802	0.9318	0.8017	0.5712	0.3525
	NCC	1	1	1	0.9994	0.9150
Barbara	SSIM	0.9823	0.9394	0.8261	0.6213	0.3975
	NCC	1	1	1	0.9997	0.9425

Now, we pass the watermarked images (Lena and Barbara) to different attack such as JPEG compression, Noise salt & pepper, Gaussian noise. Image color resists to the attack if we compare with image gray level. Recovered mark/secret doesn't have more difference with original mark when has a value important. It cannot be exceeding 50 because the extracted image is starting to degrade. TABLE II and TABLE III show NCC value after attacking Lena and Barbara image watermarked.

TABLE II. NCC VALUE USING LENA AS MEDIUM

Attack / α	5	10	20	40	80
JPEG compression	0.9135	0.9262	0.9972	0.9988	0.9089
Noise salt & pepper	0.8595	0.8976	0.8994	0.8799	0.8851
Gaussian noise	0.7824	0.7918	0.8377	0.8997	0.8927

TABLE III. NCC VALUE USING BARBARA AS MEDIUM

Attack / α	5	10	20	40	80
JPEG compression	0.9120	0.9259	0.9944	0.9933	0.9127
Noise salt & pepper	0.8121	0.8944	0.9201	0.9404	0.8933
Gaussian noise	0.7938	0.8516	0.8639	0.8813	0.8901

V. CONCLUSION

One algorithm can manage steganography and watermarking operations by specifying the appropriate value of the reference parameter and reference matrix . Highest SSIM is required to avoid a doubt of watermark image presence in medium for steganography. By increasing , we move to watermarking and the mark takes a role of protecting the medium. It is evident that SSIM is decreased however the quality of extracted watermarked image is still better except if is very important. Color image resists to the attack because we don't touch red and green channel. We are able to read the message even noise is present but NCC value is always acceptable.We can call this application to protect an artwork or transmitting a secret image through internet. This algorithm can be extended to encrypt a numeric image.

REFERENCES

[1]. J. Eloff, T. Morkel, M. Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[2]. F. Rahmanti ,P. Adi, "Image Watermarking on Low Frequency DWT Using Singular Value Decomposition and Dither Quantization," Seminar Nasional Teknologi Informasi dan Komunikasi 2016 (SENTIKA 2016), Yogyakarta, 18-19 Maret 2016.

[3]. J. Liu , X. Sun, J. Sun, Q. Zhang and W. Ji, "A Robust Image Watermarking Scheme Based on the Relationship of SVD," 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, 2008, pp. 731-734, doi: 10.1109/IIH-MSP.2008.190.

[4]. A. Melman, R. Meshcheryakov, O. Evsutin, "Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions," in *IEEE Access*, vol. 8, pp. 166589-166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[5]. R. Gomathi, S. Aiswarya, "Review On Cryptography and Steganography Techniques in Video," *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, India, 2018, pp. 1-4, doi: 10.1109/ICCIC.2018.8782409.