BEMD-HT Based RGB Color Image Robust Information Hiding Algorithm Using Block Averaging Technique

Most. Shelina Aktar^{1*}, K.M. Ibrahim Khalilullah², Shugufta Abrahim³ and Md. Ekramul Hamid¹

 ¹Department of Computer Science and Engineering, University of Rajshahi, Rajshai-6205, Bangladesh
 ²PhD Research Fellow, Graduate School of Science and Engineering for Education, Toyama University, Toyama, Japan
 ³Department of Computer and Information Systems, Jazan University, Jazan 45142, Saudi Arabia
 *amostshelina@yahoo.com

Abstract

The paper proposes an information hiding technique for steganography and digital watermarking using Bi-dimensional Empirical Mode Decomposition (BEMD) and Hilbert Transform (HT). We use RGB color image as a cover image. The cover image is divided into a number of blocks. Then each block of the cover image is putrefied into a number of Intrinsic Mode Functions (IMFs) using BEMD. We embed secret information with private key into a significant IMF. The embedded secret information, called watermark, is a matrix of 1 and -1. However, this watermark is generated by mapping pseudo-random numbers. Therefore, any unauthorized person who does not possess the private key cannot extract the watermark. The significant IMF is a highest energetic IMF which is selected according to the energy distribution of the putrefied IMFs. Thus the selected IMF is less sensitive to common image and signal processing manipulation. In watermark extraction process, we transform the watermarked object into frequency domain using HT bypassing the use of BEMD due to its empirical characteristics. Thereafter, we extract the watermark bit using block averaging technique. The experimental results of this algorithm demonstrate that the proposed method has better imperceptibility and it is more robust against several image processing and geometric manipulations.

Keywords: Steganography, HT, BEMD, PSNR, IMF, Watermarking, Block Averaging Technique

1. Introduction

The growth of Internet, new technologies, and new applications has made entertainment industry, government intelligence, and police agencies nervous. This threat forces us to invent new protection mechanism. One of the newest topics in multimedia and Internet security research is information hiding. Steganography and watermarking are two important sub-discipline of information hiding. Steganography is the art and science of secret communication that hides the existence of communication. Steganography technique is used to hide message or secret information into another harmless object or media like image, audio, and video such that any enemy cannot detect that there is a second message present [1]. As opposed to steganography, digital watermarking has additional requirements of robustness against possible manipulation on watermarked object. Digital watermarking is a process to watermark into multimedia object, called

^{*}Corresponding Author

cover or host object, such that watermark can be extracted or detected later to make an assertion about the object [1]. There are two common approaches for embedding watermark into host object popularly known as spatial domain and transform domain. It is a relatively easy process to embed into the spatial domain but less robust against common signal processing manipulations. On the contrary, the transform domain method is more robust against various signals processing manipulation than spatial domain method. Digital watermarking has become an integral part in many fields of multimedia and Internet security due to its important functions and applications. It has been used in digital content for verification and copyright protection. A number of other recommended applications are [1]: broadcasting, transaction tracking, content authentication and tamper detection, fingerprinting, and information carrier. The relationship among cover object, secret information, and

Minghui and Jingbo proposed an image watermarking technique based on Bidimensional Empirical Mode Decomposition (BEMD) [2]. They select the intermediate frequency of the IMF to add watermark. Benkuider and Aarab used BEMD technique by applying additive watermarking scheme on each Bi-dimensional Intrinsic Mode Function (BIMF) [3]. Ning et. al., proposed a multiband wavelet transformation (MWT) and EMD approach to embed the watermark into the average trend of coefficients of some middlefrequency sub bands in wavelet domain [4]. Huang and Sun proposed the HVS model using IMFs [5]. A chaos-based watermarking algorithm is introduced by Hei and Zhu where they extracted the watermark by calculating the sum of statistic of the coefficients from watermarked image [6]. Wenjuan and Hongmei proposed a DWT-SVD technique to increase the level of robustness of the watermarked image [7]. Wang et al. used LU Factorization to embed watermark in wavelet domain [8]. From the experimental results of the above papers, we see that some of them are good for common image processing manipulations and some of them are good for geometric attacks, but not for both. Due to matrix multiplication operation during watermark extraction process, the SVD and LU based watermarking techniques are very sensitive to geometric and common signal processing manipulation.

In this paper, we propose BEMD-HT based information hiding technique for steganography and digital watermarking. The BEMD decomposes the input signals into a series of IMFs and then select a significant IMF to embed watermark. In wavelet transform domain technique, the high frequency band or the low frequency band is used to embed secret information. Due to multi-resolution analysis in wavelet domain, the size of the wavelet transform domain is reduced; therefore the whole transform domain can't be utilized to embed watermark. The conventional frequency domain filtering methods (*i.e.*, Fourier and wavelet transform) depend on the priori basis functions and hence the data is fitted with those functions; otherwise fail to fit the data perfectly. The limitations are overcome by using Bivariate Empirical Mode Decomposition. The BEMD is fully data dependent. Therefore, the BEMD does not use any basis function to fit the data. The proposed technique takes the advantage of orthogonal properties of the BEMD. In addition, the BEMD technique perfectly meets Human Visual System (HVS) [9]. Due to perfect time-frequency localization properties of BEMD, we have addressed imperceptibility situation with the use of BEMD. Most of the BEMD based techniques transform the whole object into a series of IMFs during embedding and extraction process; which is very time consuming and complex process as well as the watermarked objects are more fragile with signal processing manipulations. For this reason, BEMD-HT based block averaging technique is proposed to solve these limitations. Due to block-wise operation and significant highest amplitude spectral IMF selection process, this proposed technique is much more insensitive to general image processing manipulations when compared with other techniques [4-8].

2. Proposed Technique

The Bi-dimensional Empirical Mode Decomposition method first introduced by Huang, *et. al.,[*10]. The BEMD method permits to analyze nonlinear and non-stationary two dimensional signals. The principle of BEMD is to decompose adaptively a 2D signal into frequency components. These frequency components are called intrinsic mode functions (IMFs) that acknowledge well-behaved Hilbert transforms [10]. The IMFs are calculated from input signal by means of an algorithm called sifting process. In the proposed information hiding technique, at first the G channel is separated from the RGB color image. Then the G channel is divided into a number of blocks. Each block is decomposed into a finite set of intrinsic mode functions using BEMD. After that, the significant IMF is selected according to the energy distribution of the IMFs. Then only one bit of the watermark is added to the selected IMF of each block. In this algorithm, we pick highest energetic IMF as a significant IMF. A number of IMFs of a block of the G channel are given in Figure 1.



Figure 1. Some IMFs of a Block of the Lena Image

A matrix $\mathbf{W}(\mathbf{x}, \mathbf{y})$ with negative and positive pattern mapped from pseudo-random matrix with a specified key is added to the significant IMF as secret information by using the following additive embedding formula:

$$\mathbf{d}_{\mathbf{i}}^{\prime} = \mathbf{d}_{\mathbf{i}} + \alpha \mathbf{B} \tag{1}$$

where d_i is the selected IMF of the ith block, d'_i is the embedded IMF of the ith block, and *B* is a single value of the watermark matrix, W(x, y). The size of the matrix is $m \times n$, where

$$m = \left\lfloor \frac{S_r^h}{S_r^b} \right\rfloor$$
, and $n = \left\lfloor \frac{S_c^h}{S_c^b} \right\rfloor$ (2)

The S_r^h and S_r^b represent the number of row of the host image and number of block of the image respectively such that, $m \times S_r^b \leq S_r^h$. Similarly, the S_c^h and S_c^b represent the number of column of the host image and number of block of the image respectively such that, $m \times S_c^b \leq S_c^h$. The symbol α is a scaling factor. The value of the scaling factor should be as high as possible while remaining imperceptible of embedded watermark. The watermarked block is constructed by summing embedded IMF and all of the remaining IMF of the block. Finally watermarked image is constructed from watermarked blocks of the host image. An abstract block diagram of the embedding and extracting process of the proposed algorithm is shown in Figure 2.







(b)

Figure 2. Watermark Embedding and Extracting Process. (a) Embedding Process, (b) Extraction Process

In the watermark extraction process, the host image and watermarked image are divided into a number of blocks. Then each block is transformed into Hilbert transform domain. Then the block of same watermark bits is extracted using the following subtraction equation:

$$\mathbf{w}_{\mathbf{b}} = \left(\mathbf{H}_{\mathbf{i}}^{\prime} - \mathbf{H}_{\mathbf{i}}\right) / \alpha \tag{3}$$

where H'_i is the watermarked block in Hilbert transform domain, and H_i is the Hilbert transformed domain of ith block of the host image. Since BEMD process is empirical, there is no explanation the decomposition will result in similar IMFs when the watermarked image is manipulated (or even any secret information added). The entire scheme will fail if different result comes from the same IMFs. Therefore, we directly use Hilbert transform excluding the use of BEMD in the watermark detection process.

The resulted watermark bit is calculated by block averaging over the number of embedded watermark to the block using the following thresholding process:

$$\mathbf{W}'(\mathbf{x}, \mathbf{y}) = \begin{cases} -1, \ mean(\mathbf{w_b}) \le T\\ 1, \ mean(\mathbf{w_b}) > T \end{cases}, \text{ where } 0 \le T \le 0.5$$
(4)

Finally we get the resulted watermark after calculating the above operation for all blocks of the cover image.

The Peak Signal-to-Noise ratio (PSNR) is popularly used to measure quality of watermarked image. Most of the researchers use the PSNR for grayscale images. In this paper, we calculate PSNR for evaluating quality of the RGB color watermark image. If X(M, N, P) and Y(M, N, P) represent host color image and watermarked color image respectively, the Mean Square Error (MSE) is calculated as,

$$MSE = \frac{1}{(P \times M \times N)} \sum_{u=1}^{M} \sum_{v=1}^{N} \sum_{t=1}^{P} [\mathbf{X}(\mathbf{u}, \mathbf{v}, \mathbf{t}) - \mathbf{Y}(\mathbf{u}, \mathbf{v}, \mathbf{t})]^2$$
(5)

After that maximum values of the host image and watermarked image is calculated using the following,

$$max1 = argmax(X(M, N, P))$$
$$max2 = argmax(Y(M, N, P))$$

The value of P is 3 for RGB color images. Then choose maximum of the two values,

Peak Value = max([max1 max2])

Finally the PSNR is calculated by the following equation:

$$PSNR = 10\log\left(\frac{Peak \, Value^2}{MSE}\right) \tag{6}$$

The normalized correlation between original watermark and extracted watermark is used to measure similarity between them. The proposed technique utilizes the following equation to calculate normalized correlation:

$$\phi_{\rm NC} = \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} W(x,y) W'(x,y)}{\sqrt{\sum_{x=1}^{m} \sum_{y=1}^{n} W(x,y) W(x,y)} \sqrt{\sum_{x=1}^{m} \sum_{y=1}^{n} W'(x,y) W'(x,y)}}$$
(7)

where ϕ_{NC} is the normalized correlation, W(x, y) is the original watermark, and W'(x, y) is the extracted watermark.

In this proposed algorithm, the number of distorted bits in the extracted watermark is calculated by using the following formula:

$$\beta_{\rm N} = \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} |W'(x,y) - W(x,y)|}{2}$$
(8)

where β_N is the number of distorted bits in the extracted watermark. The accurate Structural similarity between two watermarks is calculated using the following formula:

$$\gamma_{\rm S} = \frac{\left(100 \times \left(L_{\rm W} - \left(\frac{\sum_{x=1}^{\rm m} \sum_{y=1}^{\rm n} \left|w'(x,y) - w(x,y)\right|}{2}\right)\right)\right)}{L_{\rm W}} \tag{9}$$

where γ_S represents structural similarity between original watermark and extracted watermark, and L_W is the length or size of the watermark.

3. Experimental Results & Discussion

The well-known RGB color Lena image is used to test the proposed technique. A matrix W(x, y) with negative and positive pattern mapped from pseudo-random matrix with a specified key is considered as secret information. At first the R, G, and B channels are separated from the host image. Then the secret information is added into the G channel. Therefore, the difference image reflects green color which represents watermark information. The host image, watermarked image, and their difference are shown in Figure 3.



Figure 3. Original, Watermarked, and Difference Image

The PSNR value of the unattacked watermarked image is **107.9485db**. To test the robustness of this algorithm the watermarked image is attacked by various common image processing operations and geometric transformations; such as Noise addition, filtering, compression, rotation, cropping, and morphing which have been shown below sequentially. All of the parameters are taken from Matlab functions.

3.1. Noise Addition

To measure performance of this algorithm white Gaussian noise and Salt and Pepper noise are added with different variances. The attacked watermarked images with PSNR and their performance measurement values are shown in Table 1, as an example.

Type of NoiseAttacked ImageCorrelationDistortedSimilarit (φ_{NC}) $Bits (\beta_N)$ $y (\gamma_S)$			Normalized	Number of	Structural
	Type of Noise	Attacked Image	Correlation (φ_{NC})	Distorted Bits (β_N)	Similarit y (γ_S)

Table 1. Robustness Test by Adding Noise



The performance measurement values such as number of distorted bits, PSNR, percentage of structural similarity, and normalized correlation for different variances in case of Gaussian white noise are given in Figure 4. The variance is proportional to the amount of added noise. From Figure 4, we see that the extracted watermark remain same up to the variance 0.022 as compared to original watermark and the number of distorted bits is zero (0). When the value of variance is 0.022, the normalized correlation value is of 1. From the two figures we can demonstrate that our proposed technique perform better up to the variance of 0.035 against Gaussian noise attack.



Figure 4. Performance Measurement Values for White Gaussian Noise with Different Variances; (a) No. of Distorted Bits, PSNR, and Structural Similarity, (b) Normalized Correlation

Figure 5, shows the performance measurement values for Salt and Pepper noise with different variances. From Figure 6, and 7, we see that the percentage of structural similarity is 100 up to the value of variance 0.0356. At this point, the number of distorted bits is zero (0) and the normalized correlation is one (1). From the Figure 4-7, we conclude that the proposed information hiding techniques is less sensitive to Salt and Pepper noise as compared to the white Gaussian noise.



Figure 5. Performance Measurement Values for Salt and Pepper Noise with Different Variances; (a) No. of Distorted bits, PSNR and Structural Similarity, (b) Normalized Correlation

3.2. Compression

In this experiment watermarked image is attacked by JPEG compression with different quality factors. One of the experimental results is shown in Table 2. From the Table 2, we see that this algorithm performs better even if the quality factor is 5. The performance measurement values for JPEG compression with different quality factors are shown in Fig. 6. From Figure 6, we can demonstrate that the performance of the algorithm increase when the value of the quality factor increase. From Figure 8, we see the normalized correlation, number of distorted bits, and percentage of structural similarity values are 1, 0, and 100 respectively from 15 to upper values of the quality factor.

Type of Attack	Attacked Image	Normalized Correlation (φ_{NC})	Number of Distorted Bits (β_N)	Structural Similarity (γ_S)
JPEG Compressi on with Quality=5 PSNR= 56.05db		0.84	2	92%

	Table 2.	Robustness	Test for	Compression
--	----------	------------	----------	-------------



Figure 6. Performance Measurement Values for JPEG Compression with Various Qualities; (a) No. of Distorted Bits, PSNR, and Structural Similarity, (b) Normalized Correlation

3.3. Filtering

Attacked images by various filtering and their performance measurement values are given in Table 3. The experimental results of the Table 3, demonstrate that the proposed scheme is having a very good performance even after various filtering attacks.

Type of Filtering	Attacked Image	φ_{NC}	β_N	γ _s (%)	Type of Filtering	Attacked Image	φ_{NC}	β_N	γ _s (%)
Median Filtering on G channel [3 3] PSNR= 86.64db		1.0	0	100	Average Filtering [5 5] PSNR= 62.96db		0.84	2	92
Median Filtering on G channel [5 5] PSNR= 79.58db		0.84	2	92	Image Blurring type=disk radius=20 PSNR= 48.73db	R	0.84	2	92
Gaussian Filtering [5 5] Standard deviation =0.5 PSNR= 88.29db		1.0	0	100	Linear Motion of a Camera Parameter: len=20 and theta=45 PSNR=		1	0	100

Table 3. Robustness Test for Various Filtering

				57.61db			
Gaussian Filtering [15 15] Standard deviation =0.5 PSNR= 88.27db	1.0	0	100	Sharpened Filtering PSNR= 50.34db	1	0	100

3.4. Geometric Attack

Table 4, represents different types of geometric attacks and their measurement values of the proposed information hiding technique. The following table also illustrated that the proposed algorithm performs better geometric attacks.

Type of Geometric Attack	Attacked Image	φ_{NC}	β_N	γ _s (%)	Type of Geometric Attack	Attacked Image	φ_{NC}	β_N	γ _s (%)
Image Morphing PSNR= 42.17db		0.84	2	92	Left- corner Cropping (200×200) PSNR= 37.07db		0.92	1	96
Rotation with Cropping Angle=-20		0.44	7	72	Center Cropping (100×100) PSNR= 48.41db	R	1	0	100
Surrounding Cropping (2/5) PSNR= 26.39db		0.44	7	72	Center Cropping (200×200) PSNR= 34.01db		0.68	4	84

Table 4. Robustness Test for Geometric Attack

4. Performance Comparison for JPEG Compression

In order to prove the performance of this algorithm, this paper compares Literature [212] by experiment. The above results indicate that most of the cases the proposed technique performs better than the results shown in Literature [2-12]. Zhuokang *et. al.*, [11] added the white Gaussian noise with variance 0.0001 and their correlation values is 0.8496, which is lower than the proposed algorithm. Wang et al., [8] added the noise with variance value 0.01. In the proposed technique, the correlation value is 1 even when the variance value is 0.022. Therefore, we conclude that the proposed technique perform well than the algorithm applied in the Literature [8-11] against noise attack. In DCT[11] based method, the normalized correlation is 0.7328 after Gaussian low pass filtering with the parameter 15×15 whereas the value is 1 in our proposed method shown in Table 3. The results of different types of filtering shown in Table 3, are outer perform than other methods [3-12]. In geometric attack our algorithm performs well as shown in the above

table. The compared graph for JPEG compression with different quality factor is shown in Figure 7.

From Figure 7, we see that the normalized correlation value of the proposed method is one (1) at quality factor 15 whereas the normalized correlation value is 0.9961 at quality factor 20 in case of DWT-SVD based method [7]. The results of the Figure 7, indicate that the proposed algorithm perform well than other methods applied in Literature [7-12].



Figure 7. Performance Comparison Graph for JPEG Compression

5. Conclusion

In this paper, we propose robust color image-adaptive information hiding algorithm with the use of block BEMD and averaging technique. The efficiency of this algorithm has been shown in a series of experimental results. A multiband approach is presented here for hiding information into the image. The decomposition process of BEMD uses a data adaptive time varying filtering method, and therefore the algorithm is highly efficient for perceptual transparency (imperceptibility) and robustness. The BEMD based sub band decomposition is a complete decomposition, because the selected block of the host image can easily be obtained by simply summing up the individual IMFs [10]. Due to the empirical characteristics of BEMD, we use Hilbert transform and block averaging in the extraction process which has reduced a lot of calculation complexity as compared to other BEMD based methods. With further improvement, this technique can be used in other media, such as digital video watermarking and text processing as well as can be combined with cryptography techniques for enhancing security.

References

- [1] I. J. Cox, M. L. Miller and J. A. Bloom: "Digital Watermarking", Morgan Kaufmann Publishers, (2002).
- [2] D. Mingui and Z. Jingbo, "Robust Image Watermarking Algorithm against Geometric Attack Based on BEMD", International Conference on Computer and Communication Security, Hong Kong, (2009), pp. 36-39.
- [3] A. Benkuider and A. Aarab, "Digital watermarking using Bidimensional Empirical Mode Decomposition", International Conference on Multimedia Computing and Systems, Ouarzazate, (2011), pp.1-6.
- [4] N. Bi, Q. Sun and D. Huang, "Robust Image Watermarking Based on Multiband Wavelets and Empirical Mode Decomposition', IEEE Transaction on Image Processing, (2007), vol. 16, no. 8, pp. 1956-1966.

- [5] W. Huang and Y. Sun, "A New Image Watermarking Algorithm Using BEMD Method", International Conference on Communications, Circuits and Systems, Kokura, (2007), pp. 588-592.
- [6] Xi-Ping He, Qing-Sheng Zhu: 'A Robust Wavelet-Domain Watermarking Algorithm for Color Image', International Conference on Machine Learning and Cybernetics, Dalian, China, (2006), pp. 3940 – 3943.
- [7] C. Wenjuan and Y. Hongmei: 'Watermarking Algorithm Against Geometrical Attacks Based on DWT-SVD', International Conference on Multimedia Technology, Ningbo, (**2010**), pp. 1-4.
- [8] S. Wang, W. Zhao and Z. Wang: "A Gray Scale Watermarking Algorithm Based on LU Factorization", International Symposiums on Information Processing, Moscow, (2008), pp. 598 – 602.
- [9] A. N. K. Zaman, K. M. I. Khalilullah and M. W. Islam, "A robust digital audio watermarking algorithm using Empirical Mode Decomposition", 23rd Canadian Conference on Electrical and Computer Engineering (CCECE), Calgary, AB, (2010), pp. 1-4.
- [10] Norden E. Huang, 'The empirical mode decomposition and the hilbert spectrum for non-linear and nonstationary time series analyses, Proceeding of Royal Society, London, (**1998**), pp. 903-995.
- [11] Z. Jia and Z. Ting, "The research and design of Invisible Digital Watermarking Based on DCT and Matlab", International Conference on Computer Science and Network Technology, Harbin, (2011), pp. 825 – 828.
- [12] L., Sumalatha, V. V. Krishna and M. R.: Kumar, 'A Robust Image Watermarking Scheme Using Simplified Significant Wavelet Tree Quantization', 15th International Conference on Advanced Computing Technologies, Rajampet, (2013), pp. 1-4.
- [13] M Swanson, B Zhu and A Tewfik, "Robust audio watermarking using perceptual masking', Signal Processing, (1988), 66, (3), pp. 337–355.

Authors



Most. Shelina Aktar, obtained her B.Sc. and M.Sc. degree in Computer Science and Engineering from University of Rajshahi, Rajshahi-6205, Bangladesh in the year of 2009 and 2010 respectively. She was working as a Part-time Lecturer in the department of Computer Science and Engineering, Dhaka International University, Dhaka-1205, Bangladesh. Her research interests include Image/Video quality assessment, Digital Image and Signal Processing, Pattern Recognition and Computer Vision.



K. M. Ibrahim Khalilullah, obtained his B.Sc. and M.Sc. degree in Computer Science and Engineering from University of Rajshahi, Rajshahi-6205, Bangladesh in the year of 2006 and 2007 respectively. He is a PhD student in the department of Mechanical and Intellectual Systems Engineering at Toyama University in Japan. His research interests include in Intelligent Systems, Assistive Robotics, HCI, BMI, Machine Learning, and Computer Vision.



Mrs Shugufta Abrahim, obtained her BSc in Information Technology from University of Kashmir, India in the year 2008 and M.Sc. degree in Computer Sciences from Jamia Hamdard University, New Delhi, India, in the year of 2010. She was working as Lecturer in the Department of Computer Science and

Information Systems, Jazan University, Saudi Arabia. Currently, she is PhD student in the graduate school of Science and engineering, at University of Toyama, Japan. Her research interests include Computer simulations, computer gaming, Image/Video quality assessment, Digital Image and Signal Processing, Pattern Recognition and Computer Vision, advanced mathematics and computer human interfaces.



Md. Ekramul Hamid, received his B.Sc and M.Sc degree from the Department of Applied Physics and Electronics, Rajshahi University, Bangladesh. After that he obtained the Masters of Computer Science from Pune University, India. He received his PhD degree from Shizuoka University, Japan. During 1997-2000, he was a lecturer in the Department of Computer Science and Engineering, Rajshahi University. Dr. Hamid was working as Assistant Professor at the King Khalid University, Abha, KSA from 2009 to 2011. He worked as a visiting researcher in Shizuoka university, Japan in 2012 and 2014, respectively. He is currently working as Professor and Chairman in the Department of Computer Science and Engineering, Rajshahi University. His research interests include Digital Signal Processing, Analysis and synthesis of speech signal, Speech Enhancement and Image Processing.