International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-2, December 2011

AMBTC-Compressed Image Using Genetic Algorithm

Anubhuti Khare, Manish Saxena, Heena A Jain

Abstract*: *In this paper, we present an image-hiding scheme based on genetic algorithm. The secret messages are embedded into a compressed image of AMBTC. Genetic algorithm is enveloped to find the best substitution of AMBTC bitmap. The proposed scheme provides high visual quality of the stego-image. The enhanced system of the proposed scheme increases embedding capacity while retaining good quality of the stego-image. Experimental results show that the proposed scheme outperform the comparative schemes.

Index Terms*: *AMBTC, Genetic Algorithm,

I. INTRODUCTION

As the problems of the illicit interception and illegal copying of digital media are becoming more and more serious the technique of information hiding is thus proposed to securely transmit and protect digital media without incurring the attention of unintended recipients when sending data over the Internet. The technique is different from cryptography [5]. In contrast, information hiding is about transmitting the given secret data through a cover medium in a manner that the existence of secret data is unnoticed [2]. Although there is a trade-off between the hiding capacity and the quality of the stego-medium, these two factors are considered to be the important measurements in developing data hiding systems. Among the spatial domain image hiding methods, the least significant bit (LSB) method is the simplest one [10]. In 2002, Jo and Kim proposed a watermarking scheme [6] based on vector quantization. Several image hiding methods that embed secret data in frequency domain had been proposed. In [8], a steganography method based on the discrete wavelet transformation (DWT) was presented. In addition, a scheme that embeds information in the middlefrequency of the quantized DCT was provided in [1]. In 2002, Tsai *et al.* proposed an image hiding technique using block truncation coding [9]. In this scheme, the secret message is embedded into the AMBTC compressed image. In 2000, Pan *et al.* proposed a datahiding scheme [7] for two-color images. When using those methods by which secret data are hidden in spatial domain, it usually needs to compress the stego-image before they are transmitted. Most of the proposed schemes on image hiding in spatial domain are not robust to lossy data compression. Certain lossy data compression will even change the secret data. For this reason, we shall propose an imagehiding scheme for embedding secret messages into the absolute moment block truncation coding (AMBTC) compressed image in this paper [3]. Our image-hiding scheme is based on GA, which is used to find the best substitution for the AMBTC bitmaps.

Manuscript published on 30 December 2011.
***** Correspondence Author (s)
Dr. Anubhuti Khare*, Reader, Department of Electronics and Communication, University Institute of Technology, Rajeev Gandhi Technical University, Bhopal, Email:- anubhutikhare@gmail.com, Mobile: +919425606502
Manish Saxena, Head of Electronics and Communication Department, Bansal Institute of Science And Technology Bhopal (M.P.), India, Email: - manish.saxena2008@gmail.com
Heena A Jain, M. Tech (Digital Communication), Bansal Institute of Science and Technology Bhopal (M.P.), India. Email- jainhee@gmail.com

II. PROPOSED SCHEME

In the proposed scheme, secret data is mainly hidden in the bitmap of the AMBTC compressed code. The proposed scheme is based on GA to explore the best AMBTC code combinations for embedding secret bits. After obtaining an AMBTC compressed block code, the genetic- based embedding procedure is adopted to embed secret data. The secret data is a random bit stream of '0' and '1'. The hiding capacity of each AMBTC compressed block in the proposed scheme is not fixed. Let *RV* denote the integer value of the secret data. The embedding rule is to modify the AMBTC bitmap for satisfying $RV = g \bmod 2^h$, where h is the number of embedding bits per block. The embedding procedure is finished when all bits of secret data are embedded into the AMBTC compressed code. The point is how to alter the bits in the AMBTC bitmap so that g can satisfy the above equation with minimal MSE distortion constraint. The MSE distortion is defined as the mean square errors between original host image and the stego-image. To systematically find the best solution, the mechanism of GA has been developed. The flowchart of the genetic based embedding procedure is shown in Figure 1.

A secret key can be incorporated in the embedding procedure to achieve a rudimental protection of the embedding messages. Hence only the key owner has the ability to extract the secret data. The encryption mechanism such as DES [4] can be applied here to encrypt the secret messages before they are embedded and to decrypt the encrypted secret messages after they are extracted. After embedding secret data in the

AMBTC compressed codes, one can use the AMBTC decompression procedure to obtain the stego-image. To enlarge hiding capacity

while retaining good image quality, the proposed scheme is enhanced. Additional 3-bits secret data are hidden in two-level quantization values when an AMBTC compressed block is determined to

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

be a non-smooth block. After an AMBTC compressed block code is obtained, the block type of this block will be determined. Hiding capacity for each compressed block varies with its block type. If the block is a smooth block, all the bits in the bitmap are used to embed secret messages. If the block is a non-smooth block, one bit is hidden in the bitmap and the quantization values, *low* and *high*, are additionally used to hide additional 3-bits secret data, respectively. Let *l SD* and *h SD* denote the secret data to be hidden in *low* and *high*. The procedure for hiding secret bits in *low* and *high* is described in detail as follows:

Step 1: Compute *El* = *low* mod 8 and *Eh* = *high* mod 8, where *El* and *Eh* are the module results.

Step 2: Compute *newlow* = *low* + (*SDl- El*) and *newhigh* = *high* + (*SDh-Eh*), respectively, where *newlow* and *newhigh* are the modified values of *low* and *high*.

Step 3: If *newlow*−*newhigh* > *TH* , then stop.

Step 4: If *newlow* ≥ *8*, then *newlow* = *newlow* -8, else *newhigh*= *newhigh+8*.

Step 5: Go to Step 3.

In the extracting procedure in the enhanced system of the proposed scheme, the secret messages *l SD* and *h SD* can be extracte d by computing mod 8 *l SD* *low* and mod 8 *h SD* *high* , respectively.

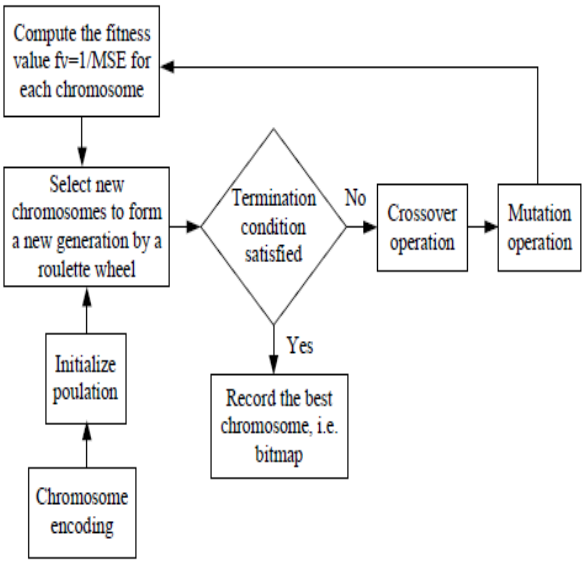


Figure 1 Flowchart of genetic-based embedding procedure

III. EXPERIMENTAL RESULT

To evaluate the performance of the proposed scheme, we have performed several simulations of the AMBTC encoded image data-embedding based on GA and compared the experimental results with those two related schemes. We compared the proposed scheme with Jo and Kim's watermarking scheme since both schemes were designed for data-embedding in the compressed domain. In both schemes, one secret data bit was block-wise embedded in an image. In Jo and Kim's watermarking scheme, four 512×512 grayscale images, namely, Lena, Man, Couple, and Woman were used to test the performance. The original image was partitioned into 16384 blocks whose size was 4×4 each. The same test images and block size were used in theproposed scheme. The grayscale image Airplane of 128 × 128 pixels was binarized and served as secret message. According to literature, the reported performance of Jo and Kim's watermarking scheme is given in Table 1. Here, *VQ PSNR* and *WM PSNR* denote the *PSNR* value of the VQ-compressed image and the value of the watermarked image, respectively. The *PSNR* is a standard way of measuring the quality of reconstruction image in image compression and so on. The four parameters used for measuring the performance of this scheme are *ED*, *HD*, *NB*, and *SR*. Here *ED* *MSE (H* H_{ga}*)* *MSE (H H* $_{ambts}$*)*, where H_{ga} and H_{ambtc} denote the genetic-based secret message embedded image and the AMBT Ccompressed image of the original image *H*,respectively.

Table 1 Performance of Jo and Kim's scheme

Images	*VQ PSNR*	*WM PSNR*	*ED*	*NB*	*SR*
Lena	31.45	30.99	5.17	15925	97.2%
Man	29.40	28.99	7.32	16245	99.2%
Couple	28.40	28.13	6.18	16101	98.3%
Woman	28.29	28.02	6.10	15848	96.7%
Average	**29.39**	**29.03**	**6.19**	**16030**	**97.85%**

Table 2 Performance of the proposed scheme

Images	*AMBTC PSNR*	*GA PSNR*	*ED*	*NB*	*SR*
Lena	34.35	34.03	1.84	16384	100%
Man	32.05	31.64	4.06	16384	100%
Couple	31.25	30.59	8.02	16384	100%
Woman	37.87	37.57	0.29	16384	100%
Average	**33.88**	**33.46**	**3.55**	**16384**	**100%**

Table 3 Estimated hiding capacities (unit: bits) of Tsai *et al*'s scheme and the enhanced system of the proposed scheme (ESPS) using different sizes of the host image

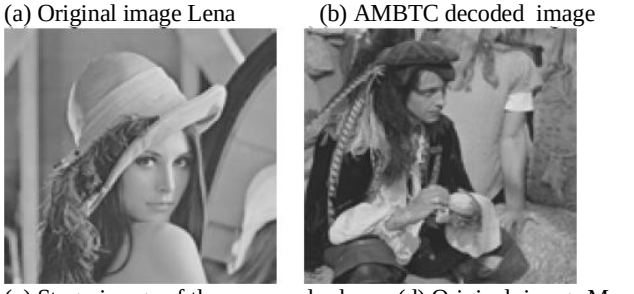
Size of the host image	Number of 4×4 blocks	Minimum capacity		Maximum capacity	
		Tsai *et al*'s scheme	ESPS	Tsai *et al*'s scheme	ESPS
64×64	256	1024	1792	4096	4096
128×128	1024	4096	7168	16384	16384
256×256	4096	16384	28672	65536	65536
512×512	16384	65536	114688	262144	262144
1024×1024	65536	262144	458752	1048576	1048576

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

HD stands for the Hamming distance between the extracted watermark bit sequence and the original watermark bit sequence. *NB* denotes the number of bits embedded, and *SR* represents the ratio of the number of watermarked blocks among all the image blocks. The performance of the proposed scheme is shown in Table 2. Here, AMBTC *PSNR* and GA *PSNR* represent the *PSNR* value of the AMBTC-compressed image and the *PSNR* value of the stego-image generated from the proposed scheme, espectively. The *HD* values are not shown in the tables of Jo and Kim's scheme and the proposed scheme because they have the same values of zeros in both schemes. From the experimental results shown above, we see that the average *PSNR* of the proposed scheme is 33.46 dB while it is 29.03 dB in Jo and Kim's scheme. Obviously, the visual quality of the stego-images that generated in the proposed scheme surpassed that in Jo and Kim's scheme. Due to the space, parts of the test images are shown in Figure 2 for visual measurement. The original images Lena and Man are shown in Figure 2(a) and 2(d), respectively. The decoded images Lena and Man are shown in Figure 2(b) and 2(e), respectively. The stego-images in Figure 2 are visual indistinguishable from their AMBTC decoded images. We compared the enhanced system of the proposed scheme with Tsai *et al*'s scheme because both schemes aim to provide high hiding capacity. In the system, the pseudo random number generator (PRNG) was used to generate the required secret messages. The test images were the same test images as those used in Jo and Kim's scheme. In Tsai *et al*'s scheme, 16 bits in the smooth block, and 4 bits in the non-smooth block are hidden when the block size equals to 16. The minimum and maximum estimated hiding capacities of Tsai *et al*'s scheme and the system using different sizes of the host images are given in Table 3.

In the enhanced system of the proposed scheme, we hide 16 bits in the smooth block, and embed 7 (3+3+1) bits in the non-smooth block where extra six bits are embedded in the two quantization levels *low* and *high*. The hiding capacities of the system are apparently larger than that of Tsai *et al*'s scheme. The maximum capacities of Tsai *et al*'s scheme are the same as ours since the extra hidden secret messages in the system are embedded in the non-smooth blocks. However, it is impossible to encounter this case in practical applications. The threshold *TH* plays an important role in controlling balance of the hiding capacity and the visual quality. The determination of the threshold value *TH* depends on user's requirement. The relationship between the hiding capacity and the threshold *TH* can be inferred as: the larger the threshold is used the higher the hiding capacity can be resulted. This inference had been confirmed in the experiment of Tsai *et al*'s scheme. To explore the relationship between the hiding capacity and the threshold *TH*, we conducted numerous experiments. Experimental results show that a higher image quality is obtained when the threshold is set to a smaller value. The visual difference between the AMBTC-decoded image shown in Figure 2 and the stego-image of the enhanced system of the proposed scheme is imperceptible. Figure 3 shows comparison of the *PSNR*s of Tsai *et al*'s scheme versus the enhanced system of the proposed scheme with test images when threshold *TH* is set 0. We obtained similar results when *TH* is set 4 or 10. According to the results, the image quality of the enhanced system outperforms that of Tsai *et al*'s scheme.

(a) Original image Lena (b) AMBTC decoded image



(c) Stego-image of the proposed scheme (d) Original image Man

(e) AMBTC decoded image (f) Stego-image of the proposed scheme

IV. CONCLUSION

In the proposed scheme, GA has been developed to find the best substitution for the AMBTC bitmaps. The stego-image is visually indistinguishable from the AMBTC-decoded images. According to the experimental results, the image quality of the proposed scheme outperforms that of Jo and Kim's scheme. The average *PSNR* of the proposed scheme is 33.46 dB while it is 29.03 dB in Jo and Kim's scheme. The hiding capacity of the enhance system is larger that of Tsai *et al*'s scheme while retaining good image quality.

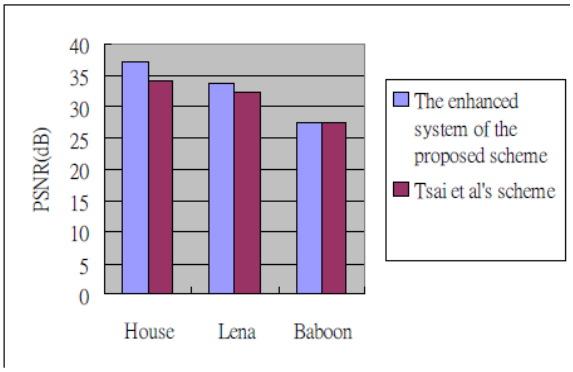


Figure 3 Comparison of the *PSNR*s of Tsai *etal*'s scheme versus the enhanced system of the proposed scheme with test images

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

REFERENCES

1. C. C. Chang, T. S. Chen and L. Z. Chung, "A steganographic method based upon JPEG and quantization table modification," *Information Sciences*, vol. 141, pp. 123- 138, 2002.
2. C. C. Chang, C. Y. Lin, and Y. H. Fan, "Lossless Data Hiding for Color Images Based on Block Truncation Coding," *Pattern Recognition*, vol. 41, no. 7, pp. 2347-2357, Jul. 2008.
3. E. J. Delp and O. R. Mitchell, "Image coding using block truncation coding," *IEEE Transactions on Communications*, vol. 27, pp. 1335-1342, 1979.
4. A. Eskicioglu and L. Litwin, "Transform domain analysis of DES," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2065-2073, 1999.
5. A. Eskicioglu and L. Litwin, "Cryptography," *IEEE Potentials*, vol. 20, no. 1, pp. 36-38, 2001.
6. M. Jo and H. D. Kim, "A digital image watermarking scheme based on vector quantisation," *IEICE Transactions on Information and Systems*, vol. E85-D, no. 6, pp. 1054- 1056, 2002.
7. H. K. Pan, Y. Y. Chen and Y. C. Tseng, "A secure data hiding scheme for two-color images," *roceedings of IEEE Fifth Symposium on Computers and Communications*, Antibes, France, pp. 750-755, July 2000.
8. J. Spaulding, H. Noda, M. N. Shirazi and E. Kawaguchi, "BPCS steganography using EZW lossy compressed images," *Pattern Recognition Letters*, vol. 23, pp. 1579- 1587, 2002.
9. P. Tsai, Y. C. Hu, and C. C. Chang, "An image hiding technique using block truncation coding," *Proceedings of Pacific Rim Workshop on Digital Steganography*, Kitakyushu, Japan, pp. 54-64, July 2002.
10. R. G. Van Schyndel, A. Z. Tirkel and C.F. Osborne, "A digital watermark," *Proceedings of theIEEE International Conference on Image Processing*, vol. 2, Austin, Texas, USA, pp. 86-90, 1994.