ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 7, July 2015

Pixel Triplet Matching Based Image Steganography for Audio Files

S. G. Shelke, S. K. Jagtap

***Abstract*—Thispaper proposes an innovative method for image steganography in spatial domain approach. This scheme is employed for embedding an audio file inside the digital images. It uses triplet pixel matching for embedding audio data covertly. The scheme improves the level of security in communication sector. In extraction algorithm audio secret data is recovered safely without distortions. Experimental results shows that proposed steganography scheme is more robust against steganographic attacks.**

***Index Terms*—embedding process, extraction process, image steganography, robustness, security, spatial domain ,stego image ,pixel pair matching, triplet pixel matching.**

I. Introduction

In recent years there is a tremendous growth in telecommunication sector. So there is a need to provide a security for all covert communications. The old way to provide security for communication is cryptography. But cryptography fails to support the robustness of a system. It just performs concealing of crucial data. Since cryptography does not hide presence of information. Drawbacks of cryptography are suppressed by the steganography. Steganography is more powerful technique in hiding secret data than cryptography. Steganography hides the crucial data inside digital kind of media like image, audio, video, internet protocols [1].

Steganography perform concealment of data using a clandestine key of any length. The similar key is used by both parties at two opposite ends of communication. Three important parameters in image steganography are cover used for embedding, key for data hiding and stego image after embedding. The party at one end of communication sends cover image with data embedded to the other party. The stego image is then received is then passed through extraction process to recover back the data concealed inside the image. But in between this communication the third user attackers would try to capture the secured data. To avoid such attacks system should be strong enough against these kinds of attacks. System should be more robust for covert communication[2].

The remainder of paper is organized as per the following sections. Section II contains literature survey in which different ways of image steganography techniques are elaborated.Section III describes methodology. Section IVshows experimental results. Section V gives the conclusion.

Manuscript received Aug 15, 2012.
S. G. Shelke, *Department of EnTC, Savitribai Phule University of Pune/ Smt. Kashibai Navale College of Engineering/ Sinhgad Institutes.,Pune, India*.

S. K. Jagtap, *Department of EnTC, Savitribai Phule University of Pune/ Smt. Kashibai Navale College of Engineering/ Sinhgad Institutes.,Pune, India*.

II. Literature Survey

The steganography mainly contains four basic domains for data embedding. They are spatial domain based approach, transform based approach, masking and filtering based approachand distortion approach. Spatial domain techniques include Least Significant Bit (LSB) hides data in least bits of cover image [3]. Pixel Value Differencing (PVD) uses differences in pixels of neighbouring placed blocks to conceal information [4]. Gray Level Modification (GLM) changes original values of intensities for embedding [5]. Parity Checker Method (PCM) employs the tool of parity checking scheme [6]. Exploiting Modification Direction (EMD) modifies pair of pixel for concealing secret information [7]. Diamond Encoding (DE) has higher data concealing capacity the EMD [8]. Optimal Pixel Adjustment Process (OPAP) uses LSB bits for data hiding by changing the values of higher bits. Adaptive Pixel Pair Matching (APPM) uses pair of pixel for data concealing [9].

III. Methodology

The methodology used is an extension of pixel pair matching technique. It embeds audio secret data inside digital image. It uses B ary notational system to embed the secret data. Higher the value of B larger will be the value of payload capacity. It increases the security level of communication system than that of previously developed spatial domain image steganography schemes [9]. Fig.3.1 shows the block diagram of methodology used.

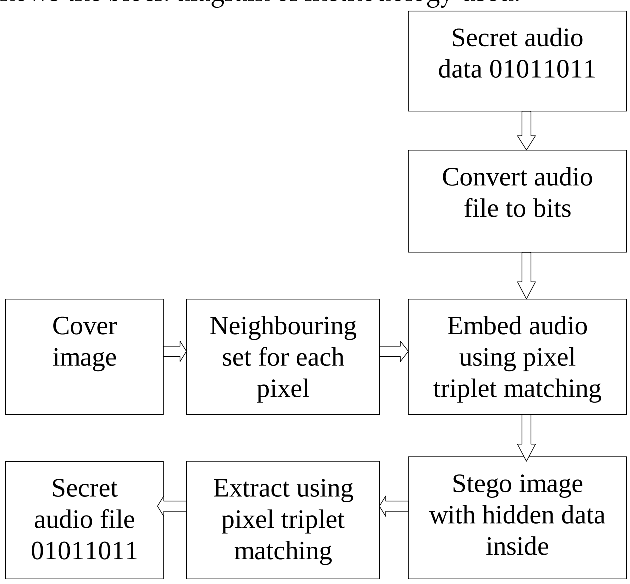

Fig. 3.1: Block diagram of methodology

The audio file is first converted into bit pattern. Using the number of bits the value of B ary is calculated. Three constants are obtained using B value. By using triplet pixel matching embedding function the audio secret file is embedded inside the digital image. The generated stego image consisting of hidden audio file is received. Extraction function of pixel triplet matching is applied over the stego image received to recover hidden audio file [10].

A. *Embedding process*

Step1: Determine the value of B ary using [10]

$$B(k) = \frac{4}{3}k^3 + 2k^2 + \frac{8}{3}k + 1 \qquad (3.1)$$

where k is called as distortion parameter.

Step2: Determine constants c_1, c_2, c_3 and neighbourhood set using the optimization rule as [10]

$$\text{Minimize: } \sum_{i=0}^{B-1} (x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2 \qquad (3.2)$$

where, $f(x_i, y_i, z_i) \in \{0,1,\ldots,B-1\}$

$f(x_i, y_i, z_i) \neq f(x_j, y_j, z_j)$ if $i \neq j$

For $0 \leq i, j \leq B-1$

Step3: Convert audio secret data into B ary notational system value

Step4: Take three pixels using and find pixels from neighbourhood set which has same embedding function value as that of secret digit in that base system. The embedding function value is determined using following function [10]

$f(x, y, z) = (c_1x + c_2y + c_3z)$ modulo B (3.3)

Step5: Replace three pixels with searched pixels coordinates.

Step6: Repeat entire procedures until all audio bits are get embedded inside image.

B. *Extraction process*

Step1: Calculate B value.

Step2: Encode secret bits to B ary notational system.

Step3: Using key generate non repeated pseudorandom sequence.

Step4: Take three pixels using and find pixels from neighbourhood set which has same embedding function value as that of secret digit in that base system.

Step5: Repeat the steps 2 and 3 until all data get extracted from image.

Step6: The audio data is recovered back by converting it back into binary pattern.

IV. RESULTS AND DISCUSSION

This section shows experimental results obtained using proposed scheme. The proposed scheme is applied on standard 512×512 two images. Two standard images used for proposed method are shown in Fig. 4.1.

Fig. 4.1: Standard images a)boat b)airplane

The audio file used has following specifications as shown in Table 1.

Table 1. Specifications of secret audio file

Specifications	Values
File name	Sample1.wav
File size	2 KB
Sampling rate	11025 Hz

Performance results of methodology used for both standard images are shown in following Fig. 4.2.and Fig. 4.3.

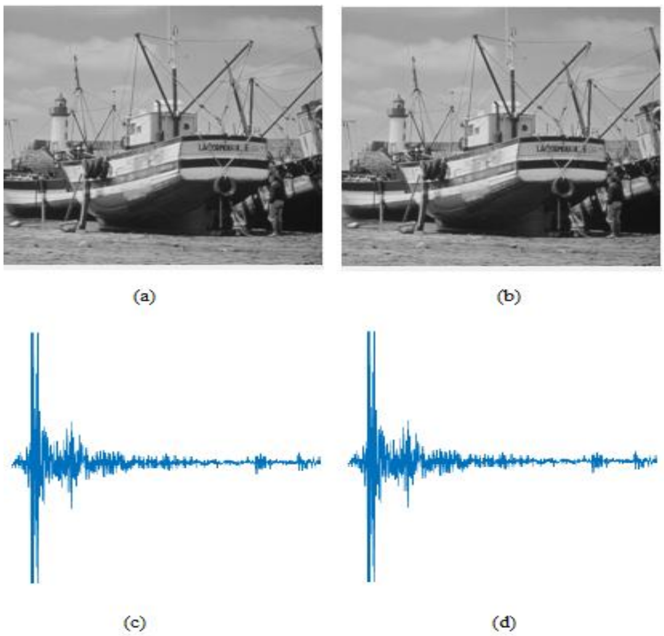

Fig. 4.2: Results for boat image a)original boat image b)embedded image c)embedded audio d)extracted audio

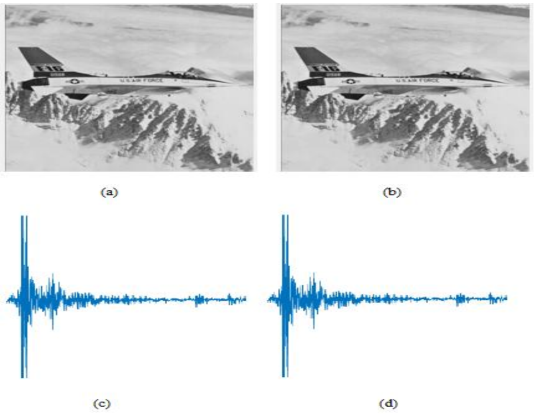

Fig. 4.3: Results for airplane image a)original airplane image b)embedded image c)embedded audio d)extracted audio

To check the quality the image between original cover image and stego image Peak Signal to Noise Ratio (PSNR) is calculated. Mean Square Error (MSE) is calculated as

$$MSE = \frac{1}{M \times N}\sum_{i=0}^{M}\sum_{j=0}^{N}(p(i,j) - p^{'}(i,j))^2 \qquad (4.1)$$

where M×N denotes the image size, $p_{i,j}$, $p_{i,j}^{'}$ and denote the values of the original image and the stego image, respectively. PSNR is then defined on a logarithmic scale in decibels.

$$(4.2) \qquad PSNR = 10\log_{10}(\frac{255^2}{MSE})$$

Test of robustivity is performed under salt and pepper noise. To test robustness of a system Noise Cross Correlation (NCC) factor is calculated using following function.

$$NCC = \frac{\sum_{i=0}^{m}\sum_{j=0}^{n} p(i,j)p'(i,j)}{\sqrt{\sum_{i=0}^{m}\sum_{j=0}^{n}|p(i,j)|^2}\sqrt{\sum\sum|p'(i,j)|^2}} \qquad (4.3)$$

A. *Before attack results*

Table 2.Boat and airplane images results before attacks

Images	PSNR	NCC
Boat	54.09	1
Airplane	54.14	1

B. *After attack results*

To check robustness of a system under attack salt and pepper noise is chosen. Robustivity is capability of a system to withstand against the unauthorized user attacks. The salt and pepper noise is most of the times get observed in images. Fig. 4.4 and Fig. 4.5 shows results of two images under salt and pepper noise.

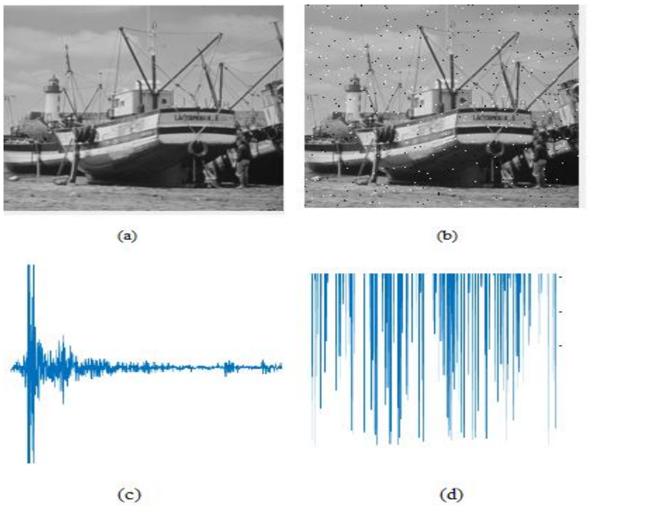

Fig. 4.4: Results for boat image a)original airplane image b)stego image with noise c)original audio signal d)noisy audio signal

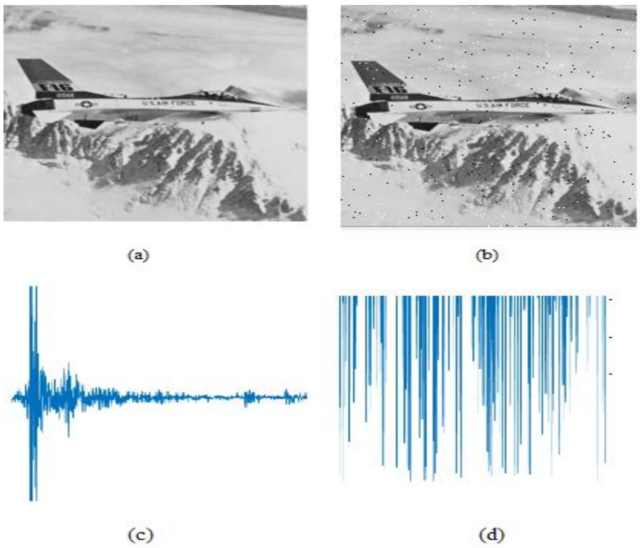

Fig. 4.5: Results for airplane image a)original airplane image b)image with noise c)original audio signal d)noisy audio signal

Due to effect of salt and pepper noise PSNR and NCC values get affected. PSNR and NCC values after salt and pepper attack are reduced after attack. Simulation results for two images under attack are given in Table 3.

Table 3.Boat and airplane images results after attacks

Images	PSNR	NCC
Boat	25.26	0.9951
Airplane	24.95	0.9954

V. CONCLUSION

The proposed scheme shows high value of PSNR. This shows the quality of embedded image is good. There is no difference is observed in between cover image and the stego image. It is also resilient to steganalysis. The best possible audio signal is retrieved under attack. Experimental results show the tradeoff between robustivity of a system and security.

ACKNOWLEDGMENT

I would like to thank my beloved and respected guide Prof. (Dr.) Sonal K. Jagtap for her encouragement and support. I gratefully acknowledge her for imparting me valuable basic knowledge of Digital Image Processing. We are also thankful to the department of Elec. and Comm., Smt. Kashibai Navale College of Engineering, Pune for providing us infrastructure facilities and moral support.

REFERENCES

[1] T. P. Morkel, J. H.Eloff and M. S.Olivier, "An Overview of Image Steganography," *inProceedings of the Fifth Annual Information Security South AfricaConference(ISSA2005)*, Jul. 2005.

[2] C. Gayathri , V. Kalpana , "Study on Image Steganography Techniques," *International Journal of Engineering and Technology* (*IJET*), vol. 5, no. 2, Apr. 2013.

[3] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.* , vol. 37, no. 3, pp. 469-474, 2004.

[4] D. C. Wu and W. H. Tsai., "A steganographic method for images by pixel value differencing," *Pattern Recognition Letters*, vol.24, pp. 1613-1626, 2003.

[5] V. Potdar, E. Chang, "Grey Level Modification Stegnography for Secret Communication," *2nd IEEE International Conference on Industrial Informatics INDIN*, May. 2004.

[6] Yadav, Rajkumar, Rishi, Rahul, Batra, Sudhir, "A new Steganography Method for Gray Level Images using Parity Checker," *International Journal of Computer Applications*, vol. 11, no. 11, Dec. 2010.

[7] K. H. Jung, K.Y. Yoo, "Improved Exploiting Modification Direction Method by Modulus Operation," *International Journal of Signal Processing, Image Processing and Pattern* vol. 2, no. 1, Mar. 2009.

[8] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP J In! Security*, vol. 2009, 2009.

[9] W. Hong and T.S. Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching," *IEEETransactions on Information Forensics and Security*, vol. 7, Feb. 2012.

[10] R. Sunder, P. Eswaran, A. Nagalinga Rajan, S Poonkuntran " High Capacity Data Embedding in Images by Pixel Triplets Matching," *International Journal of Computer Applications* ,vol. 73, no.13, Jul. 2013.

S. G. Shelke
Supriya Shelke was born in 1991. She has received B. E degree in Electronics and Telecommunication Engineering from Finolex Academy of Management Technology, Mumbai University in 2012 and currently perusing her M.E degree in Electronics and Telecommunication with specialization in Signal Processing from Smt. Kashibai Navale College of Engineering, Vadgaon(BK), Pune in Savitribai Phule Pune university.

S.K.Jagtap
Prof. (Dr.) Sonal K. Jagtap was born in 1977. She received B.E. degree in Electronics and Telecommunication Engineering in 1999. She has also completed M.E. degree with specialization in Microwave Engineering from COEP, Pune University in 2002. She had completed Ph.D. in Electronics Engineering from Shivaji University, Kolhapur in 2014.
She joined as a lecturer in E&TC in Govt. Polytechnic Osmanabad in 1999. Then to Tuljabhavani College of Engg in 2000,then to G.S. Moze COE,Pune. Presently she is working as a Assistant Professor, Smt. Kashibai Navale College of Engineering, Vadgaon(bk), Pune since 2003. She is having 15 years of teaching experience. She has till now 2 national and 22 international journal publications in her credit. She has attended and presented 20 papers in International and 12 papers in National conferences.