Available online at www.elixirpublishers.com (Elixir International Journal)

Digital Processing

Elixir Digital Processing 114 (2018) 49488-49491

ISSN: 2229-712X

A Hybrid Approach for Secure Message Communication and Color Image Watermarking

Mahimn Pandya[1] and Ashish Jani[2]

[1]Smt. K.B. Parekh College of Computer Science, M. K. Bhavnagar University.

[2]P.P. Savani School of Engineering P.P. Savani Univrsity.

ARTICLE INFO

Article history:

Received: 29 November 2017;

Received in revised form:

24 December 2017;

Accepted: 5 January 2018;

Keywords

Steganography,
Digital Watermarking,
MP-1,
Information Hiding,
Secret Communication,
Authentication,
Watermark,
Security.

ABSTRACT

This research work is nominated for an image protection technique in the area of spatial domain based digital watermarking and steganography. The proposed work has evolved a hybrid algorithm, Namely, MP-1. In this paper, a new data hiding and digital watermarking algorithm based on image matrix vectorization is provided. Experimental results show that the research work has achieved few of targeted goals such as good concealment ability, large embedding capacity. The proposed algorithm can be widely used in area of spatial domain based digital watermarking and steganography.

1. Introduction

Steganography and watermarking are employed for hiding information in a manner that only the recipient/owner can detect the existence of the secret message/watermark. Spatial domain based embedment technique is highly used in steganography as well as a watermarking system because of payload capacity. The level of secrecy is increased when novel algorithms are developed in the field of steganography and watermarking [1]. The researchers [2] have given algorithms that are applied in both steganography and digital watermarking area. In steganography, the secret information remains concealed in an envelope without it being in the notice of the eavesdropper.

The digital watermarking technique has its use to keep ownership issue intact by safeguarding the integrity of the image [3, 4 and 5]. This research work has its focus on an algorithm for good payload, imperceptibility and level of secrecy in message communication and robustness in watermark through public infrastructure channel with an objective to safeguard message or watermark.

2. Related Work

Different algorithms have so far been used to embed a watermark or secret message on the digital assets such as image, video, audio, text [2, 3, 4, 5 and 6].The digital images are frequently used for hiding data because of their payload capacity. The earlier works reported in spatial domain has adopted text-based transformation and applied to achieve an improved level of secrecy. This seeded the idea of image-based transformation for further improvement in the secrecy level [7, 8, 9, 10, 11 and12]. The similar work with encryption and decryption has reported a bit improvement in the imperceptibility [13,14 and15].

3. Proposed Work

The proposed work has a major objective is to achieve imperceptibility and increased payload capacity. Here, image matrix transformation is employed for encryption and embedment process of digital watermark and secret message. To reveal a concealed message or watermark the reverse process has done. The proposed algorithm can be categorized spatial domain based nonblind watermarking scheme.

3.1 Image Matrix Vectorization

A linear transformation a matrix, which converts the matrix into a column vector, is called **vectorization** of a matrix. i.e., the vectorization of an $m \times n$ matrix A, denoted Vec(A), is the $mn \times 1$ column vector obtained by stacking the columns of the matrix A on top of one another:

$$\boldsymbol{vec}\ (\boldsymbol{A}) = [\boldsymbol{a}_{1,1,\dots,}\boldsymbol{a}_{m,1,\dots,}\boldsymbol{a}_{1,2,\dots,}\boldsymbol{a}_{m,2,\dots,}\boldsymbol{a}_{1,n,\dots,}\boldsymbol{a}_{m,n}]^{\mathrm{T}}$$

Here, $\boldsymbol{a}_{i,j}$ represents $\boldsymbol{A}(\boldsymbol{i},\boldsymbol{j})$ and the superscript $^{\mathrm{T}}$ denote the transpose. Vectorization expresses, through coordinates, the isomorphism $\boldsymbol{R}^{mxn} := \boldsymbol{R}^{m} \otimes \boldsymbol{R}^{n} \cong \boldsymbol{R}^{mn}$ between these (i.e., of matrices and vectors) as vector spaces.

For example 2 x 2 matrix $\begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} \\ \boldsymbol{c} & \boldsymbol{d} \end{bmatrix}$ the vectorization is

$$\text{Vec (A)} = \begin{pmatrix} \boldsymbol{a} \\ \boldsymbol{c} \\ \boldsymbol{b} \\ \boldsymbol{d} \end{pmatrix} \qquad (10)$$

3.2 Secret Message or Watermark Encryption and Embedment

At the source, the targeted or cover image has converted into a column vector. Then watermark image or secret message image has converted into a column vector. Then after the watermark or secret message image vector embed to original

Tele:
E-mail address: mahimn009@gmail.com

or cover image vector. Then embedded image column vector is converted into image matrix as shown in Fig. 1.

Here, two keys are being used. The embedded channel is used as a KEY1 and message or watermark image matrix size m x n is used as KEY2. These keys are sent at destination end separately. Also, it is necessary to have a smaller image size of message or watermark in a linear relationship with the size of targeted or cover image.

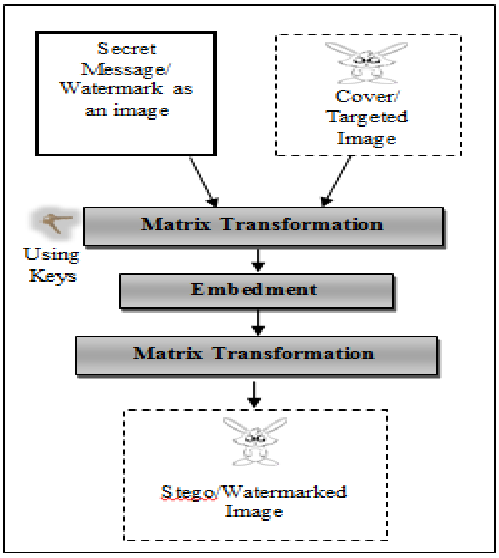


Fig. 1 Secret Message or Watermark Encryption and Embedment Process

3.3 Secret Message or Watermark Encryption and Embedment Algorithm

Step -1 Read cover or targeted image.
Step-2 Read message or watermark image.
Step-3 Convert message or watermark image into grayscale image.
Step-4 Convert message or watermark image matrix into a column vector.
Step-5 Select cover or targeted image's one color channel from RGB (Red Green Blue).
Step-6 Convert selected channel matrix into column vector.
Step-7 Embed the column vector of message or watermark to the vector of cover or targeted image's color channel.
Step-8 Convert embed channel column vector into an image matrix

3.4 Secret Message or Watermark Decryption and Extraction

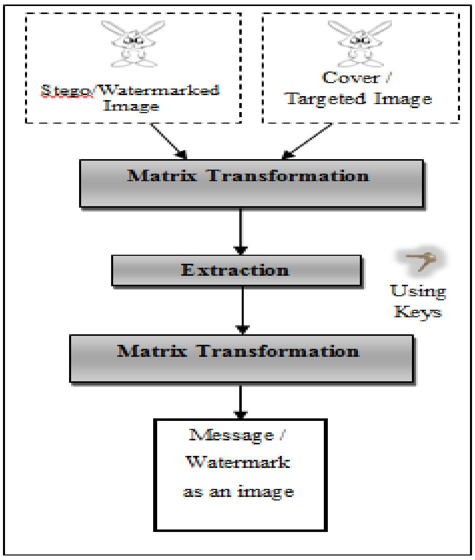


Fig. 2 Secret Message or Watermark Extraction and Decryption Process

At destination end, the watermarked or stego image, with the help of cover or targeted image, reveals the secret message or watermark by reverse the process shown in Fig. 2. Here, KEY1 is used to detect embedded channel and KEY2 is used to revel watermark or secret message.

3.5 Secret Message or Watermark Extraction and Decryption Algorithm

Step-1 Read Stego or Watermarked image.
Step-2 Read cover or targeted image.
Step-3 Convert stego or watermarked image's color channel matrix into column vector (using KEY1).
Step-4 Convert cover or targeted image's color channel matrix into column vector (using KEY1)
Step-5 Extract message or watermark column vector from the color channel of stego or watermarked image by subtracting cover or watermarked image from it.
Step-6 Convert extracted column vector into message or watermark image matrix(using KEY2).

4. Results and Discussion

The algorithm has experimented in SciLab environment. The experimental result shown here has high-resolution cover or targeted image and low-resolution watermark or message image. The size of message or watermark image used here is 256 x 256 pixels.

The cover or targeted image before embedment of a secret message or watermark is shown in Fig. 3. The message or watermark image of 128 x 128 pixels is shown in Fig. 4. And the Fig. 5 shows the resultant stego or watermarked image after applying the algorithm. The images are shown in Fig. 3 and Fig. 5 have no difference in the context of Human Visual Sense (HVS). Secondly, the histogram of a color channel of the image before and after embedment of message or watermark has shown in image Fig.6 and Fig. 7 respectively. Thirdly, the 8 x 8 matrix of image's color channel before and after embedment is shown in Table 1 and Table 2 respectively. This image matrix is changed with a minor difference and which is not noticeable. Such a way the results have proven targeted impressibility.

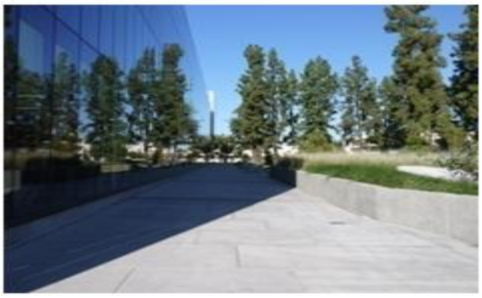
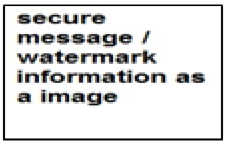


Fig.3 Cover or Targeted Image of 750 x 1000 pixels.



secure message / watermark information as a image

Fig.4 Message/Watermark Image of 128 x 128 pixels

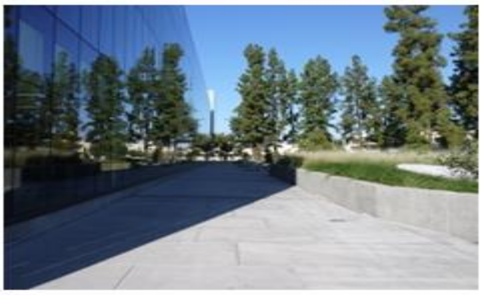


Fig.5 Stego/Watermarked Image of 750 x 1000 pixels

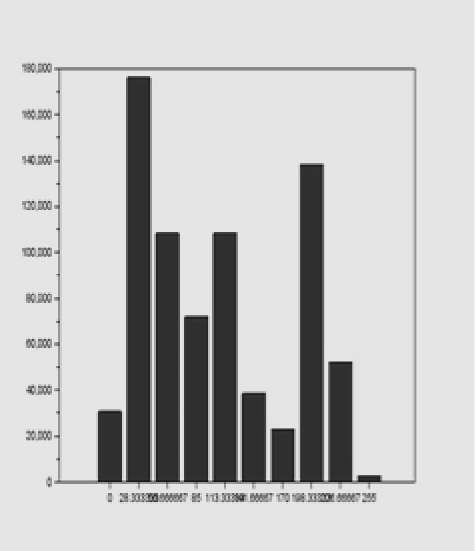


Fig.6 Histogram of Cover/Targeted Image red channel

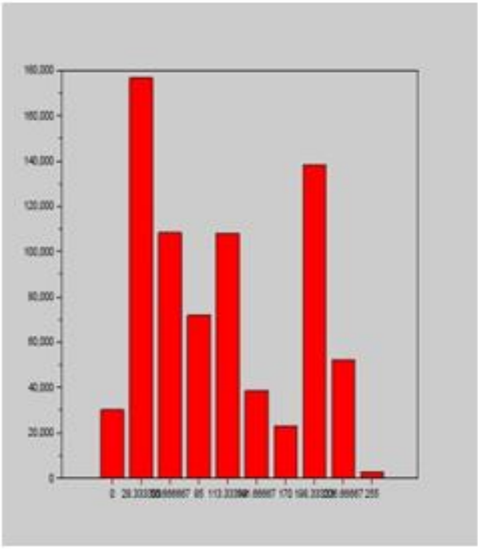


Fig.7 Histogram of Stego/Watermarked Image embedded channel (red)

Table 1. 8x8 Pixel Matrix of Cover/Targeted Image before embedment

19	22	20	17	19	21	22	24
17	19	19	19	21	21	20	21
16	16	16	17	20	19	17	18
20	19	16	17	19	18	17	20
23	21	19	19	21	20	18	22
21	21	19	19	20	20	18	21
21	22	18	16	17	18	17	18
25	25	19	14	15	17	17	15

Table 2. 8x8 Pixel Matrix of the embedded channel of stego Image (channel red)

18	20	19	20	17	22	19	23
16	17	18	17	19	20	19	20
15	15	14	109	18	18	15	17
19	18	15	21	17	17	15	19
22	20	18	15	213	19	16	21
20	20	18	17	150	19	16	20
20	21	16	14	14	17	16	17
24	24	22	12	216	16	16	14

6. Conclusion

The analysis of the results reveals that the impressibility is achieved up to some extent without high degradation of cover or targeted image is not affected. The core logic of the proposed algorithm the embedded watermark or message is scattered through the cover image that makes more difficult to detect message or watermark. This enhances the robustness of the digital watermark or message. The limitation of this work is the message or watermark image is restricted to the size of 256x256 pixels. The proposed algorithm, MP_1, used only one color channel of a cover image but the work can be extended by employing all three color channels to enhance secrecy level and payload capacity. In future, the algorithm can be optimized using TLBO [17].

Acknowledgment

The researchers are grateful to Dr. N. N. Jani for providing their guidance when experimentation and implementation of research work undertaken by giving his valuable time.

References

1. Sha, Feng, Felix Lo, Yuk Ying Chung, Xiaoming Chen, and Wei-Chang Yeh. "A Novel Optimized Watermark Embedding Scheme for Digital Images." In Multimedia Modeling, pp. 208-219. Springer International Publishing, 2015..

2. Giri, Kaiser J., Mushtaq Ahmad Peer, and P. Nagabhushan. "A Robust Color Image Watermarking Scheme Using Discrete Wavelet Transformation.", I.J. Image, Graphics and Signal Processing, pp. 2015, 1,

3. Yang, Xiao Hui, Xin Chun Cui, Zhen Liang Cao, and Zi Qiang Hu. "A Novel Digital Watermark Algorithm Based on a Fingerprint Image." In Applied Mechanics and Materials, vol. 731, pp. 173-178. 2015.

4. Goel, Savita, Shilpi Gupta, and Nisha Kaushik. "Image Steganography–Least Significant Bit with Multiple Progressions." In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, pp. 105-112. Springer International Publishing, 2015.

5. Ghebleh, M., and A. Kanso. "A robust chaotic algorithm for digital image steganography." Communications in Nonlinear Science and Numerical Simulation 19, no. 6 (2014): 1898-1907.

6. Sarkar, Tanmoy, and Sugata Sanyal. "Digital Watermarking Techniques in Spatial and Frequency Domain." arXiv preprint arXiv:1406.2146 (2014).

7. Bansal, Sonia, and Sandeep Dalal. "A Study on Digital Image Steganography and Watermarking." Biometrics and Bioinformatics 6, no. 6 (2014): 145-148.

8. Shi, Yun Qing, Hyoung-Joong Kim, and Fernando Pérez-González. Digital Forensics and Watermarking. Springer, 2014.

9. Lo, Chun-Chi, and Yu-Chen Hu. "A novel reversible image authentication scheme for digital images." Signal Processing 98 (2014): 174-185.

10. Shen, Shuyuan, Lihong Huang, and Qinglong Tian. "A novel data hiding for color images based on pixel value difference and modulus function."Multimedia Tools and Applications (2014): 1-22.

11. Hawlader, Md, Abul Kayum, Md Moniruzzaman, and Md Hossain. "A novel robust blind digital watermarking scheme based on blocking probability." In *Electrical Engineering and Information & Communication Technology (ICEEICT), 2014 International Conference on*, pp. 1-6. IEEE, 2014.

12. Pandya, Mahimn, Hiren Joshi, and Ashish Jani "Text Files Embedment to Digital Grayscale Images as Digital Watermarks and Secret Messages for Steganography" Journal of SCI-TECH Research Volume – IV, Issue – I (Jan – June 2013)

13. Pandya, Mahimn, Hiren Joshi, and Ashish Jani. "A Bespoke Technique for Secret Messaging." *International Journal of Computer Network & Information Security* 5, no. 5 (2013).

14. Pandya, Mahimn, Hiren Joshi, and Ashish Jani. "A Novel Digital Watermarking Algorithm using Random Matrix Image." *International Journal of Computer Applications* 61, no. 2 (2013): 18-21.

15. Yang, Ching-Yu. "Robust Watermarking Scheme for Colour Images Using Radius-Weighted Mean Based on Integer Wavelet Transform." In *Genetic and Evolutionary Computing*, pp. 135-145. Springer International Publishing, 2014.

16. Li, Bin, Junhui He, Jiwu Huang, and Yun Qing Shi. "A survey on image steganography and steganalysis." *Journal of Information Hiding and Multimedia Signal Processing* 2, no. 2 (2011): 142-172.

17. Jani, Ashish, Vimal Savsani, and Abhijit Pandya. "3D affine registration using teaching-learning based optimization." *3D Research* 4, no. 3 (2013): 1-6.