DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5489

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A NOVEL ALGORITHM FOR INFORMATION HIDING

Mahimn Pandya
Smt. K.B. Parekh College of Computer Science
M.K. Bhavnagar University,
Mahuva, India

Ashish Jani
P.P. Savani School of Engineering
P.P. Savani University
Surat, India

Abstract: This research paper introduces a novel algorithm can be applied either, in the area of digital watermarking and steganography, separately or together. This amalgamated algorithm, MP_2**,** is evolved for enhancement of secrecy level of a confidential message communication and imperceptibility of a watermark in the digital steganography and watermarking domain. The research work has employed matrix transformation technique to evolve embedment and encryption algorithm. This algorithm is classified in the reversible algorithm in the area of digital watermarking technique steganography.

Keywords: Steganography, Digital Watermarking, MP_2, Information Hiding, Private Communication, Authentication, Watermark, Security

I. INTRODUCTION

Nowadays in the public channel, it is very easy to re-distribute digital assets without owner's consent. Similarly, private communication through internet is also a big challenge to safeguard the confidential message from an eavesdropper. The research work is targeted to solve both the issue through one algorithm. The proposed algorithm will be applied to digital color image watermarking and steganography. The main target of the research work is to allow only the authorized person to disclose the confidential message or watermark.

The proposed embedment method is spatial domain based and used in many digital Steganographic and watermarking techniques distinctly, because of their payload capacity. In data hiding, secrecy level of message or watermark can be increased by enhancing complexity level of embedment. The evolved algorithm is not easy to decrypt for detection of embedded confidential message or watermark. The research paper introduces a novel algorithm for color image watermarking[1]–[10]

II. RELATED WORK

The researchers have given algorithms used to embed information for private messaging and digital watermarking. The digital assets like color images are protected by a watermark. Similarly, different spatial domain based algorithms evolved for the secret message communication using the digital color images as a cover medium. The researcher used color digital images often used for information hiding because of their imperceptibility level, payload capacity, and easy availability. The related works stated have adopted text-based transformation and targeted to achieve better confidentiality. They carry out the clue of image transformation for further improvement in the secrecy level[11]–[14]. The encryption and embedded method of previous research has targeted a bit improvement in the confidentiality level. The grayscale images were targeted in this work. The researchers have given watermarking techniques for color images also but not in context with confidentiality level. The research work focuses on robustness watermarking scheme[15] The research[16] was targeted only one color channel of an image but they suggested work extension by targeting all three channels to increase payload capacity and enhance secrecy level.

III. METHODOLOGY

The review findings of the related works emphasize that it's necessary to improve secrecy level. The proposed work has its focus towards the color image based watermarking and steganography technique. The image transformation is employed to increase secrecy level. The color channel is also used as a key to increasing secrecy level in confidential message communication. That is why the color images are suggested as cover images. The proposed work uses up to three color channels of an image to increase payload capacity and enhance secrecy level. The research paper aims at achieving imperceptibility and good PSNR value.

A. Matrix Transformation

A transpose of an image matrix is the resultant matrix generated by replacing all elements a_{ij} with a_{ji}. The matrix transpose is denoted by A^T. The matrix obtained by exchanging A's rows and columns and satisfies the identity

$$(A^T)^{-1} = (A^{-1})^T \qquad (19)$$

B. MP_2 Algorithm for Information Hiding

The proposed algorithm MP_2 having two sub-algorithms: first, Matrix Transformation Encryption and Embedment Algorithm (MTEEA), second, Matrix Transformation Extraction and Decryption Algorithm (MTEDA) have been used by sender and receiver respectively. The MTEEA has two inputs: first, is message/watermark an image and second is cover images for information hiding or targeted image for watermarking. The MTEEA uses a message/watermark as an image. This message/watermark image is transformed matrix to a column vector. In the same manner, the algorithm converts any required numbers of color channels of cover / original image into a column vector one by one. Thereafter, message/watermark resultant data is embedded into cover/original image. The stego image is sent to the recipient. The MTEE algorithm process is shown in figure 1. The similar numbers of inputs are used by MTEDA, shown in figure 2. The first input is stego/watermarked image and

the second input is a cover/original image. In this algorithm message/watermark is extracted by the recipient using first and second inputs. Then Key2 is applied to decrypt message/watermark. The color channel and message/watermark image size are symmetric keys used for embedment and extraction, encryption and decryption respectively. Figure 1 and Figure 2 shows the process flow of MTEEA and MTEDA, respectively.

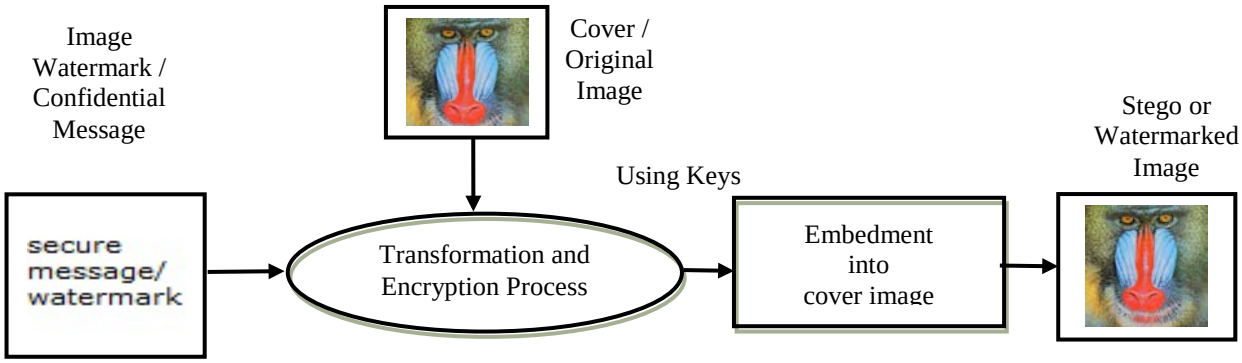

Figure 1. Matrix Transformation Encryption and Embedment Algorithm Process Flow.

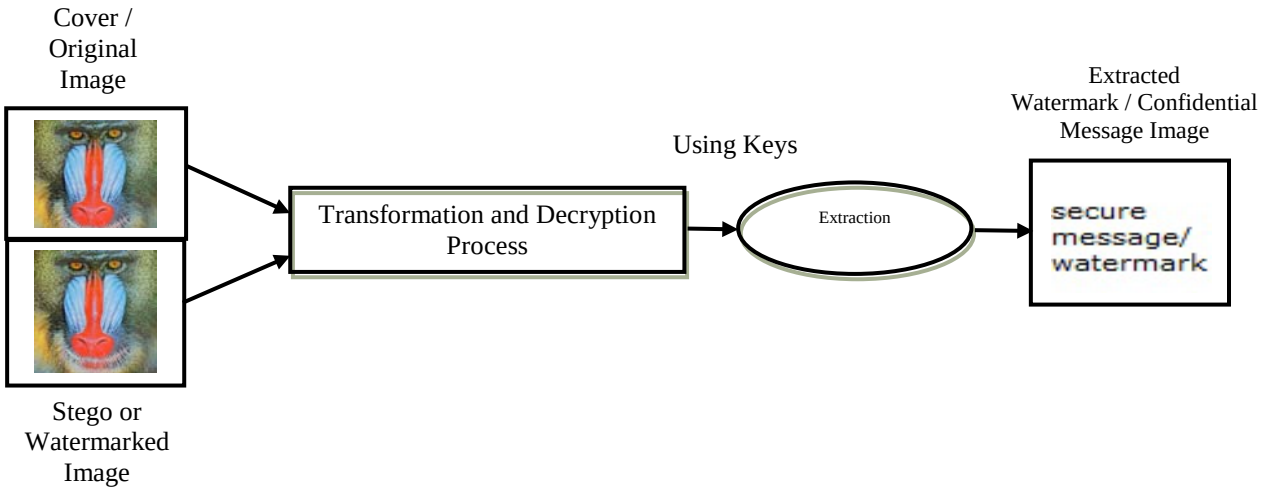

Figure 2. Matrix Matrix Transformation Extraction and Decryption Algorithm Process Flow

The method of message/watermark encryption process takes place by converting the matrix to column vector and then after it is embedded to cover/targeted image. Key2 is a matrix size of a message/watermark image using it watermark is embedded. Without Key2, it is nearly impossible to know or recognize the confidential message embedded in the stego image. In the same manner, Figure2 shows how to extract the hidden information by applying Key1 and Key2 at another end. The MTEEA is used at the source, while MTEDA is used at recipient's end. At both the places, Key1 and Key2 symmetric keys are used. The keys are sent separately.

C. Matrix Transformation Encryption and Embedment Algorithm

Step -1 *Input Cover/Original image (k).*

Step-2 *Input message/watermark Image(s).*

Step-3 *Repeat step 4 to 8 while I <=Key1*

Step-4 *if message/watermark image==color image then first converts message image to grayscale.*
gs=grayscale(s)

Step-5 *Transform message/watermark image matrix*
tm [1x n] = gs [m x n, I]

Step-6 *Transform cover/original image's channel for embedment*
tk[1 x n] = k[m x n,I]

Step-7 *Embedment process of message/ watermark image into cover image/original.*
tk[1 x n] = tk[1 x n]+ tm[1 x n]

Step-8 *Substitute selected channel of cover/targeted image according to a number of channels.*
tk[1 x n].(step will be repeated according to key1)`
cimg=k;
cimg [m x n, I]=tk[m x n]

(Note: The embedment channel and message/watermark image size are used as key1 and key2 respectively; in this case, Key1 will help to know how many channels)

The size of cover/targeted image must be greater than the size of message/watermark image. It is also noticeable in the algorithm that the cover image size can be higher in a linear

relationship with the size of message/watermark image to decrease the level of perceptibility [14]-[16].

D. Matrix Transformation Extraction and Decryption Algorithm

Step -1 *Input Stego/Watermarked image (cimg).*

Step-2 *Input cover/original image (img)*

Step-3 *Repeat step 4 to 7 while I <=Key1*

Step-4 *Transform stego/watermarked image's one channel (using a Key1 number of channels), matrix (m x n) to a column vector*
tm [1 x n] = cimg [m x n]

Step-5 *Transform cover/original image's one channel's matrix (using Key1) to message/watermark extraction*
tk[1 x n] = img[m x n]

Step-6 *Apply Extraction of message/watermark from cover/watermarked image by subtracting from stego/watermarked image*
Exmsg = tk[1 x n,I] - tm[1 x n.I]

Step-7 *Write extracted message/watermark on disk*

IV. RESULTS AND DISCUSSION

The algorithm is implemented and tested against a series of color images of different sizes. The research work experiments are done in SciLab environment. The experimental results are shown in figures. Lena original image of 512x512-pixel size is shown in Figure-3(a) used as a cover/original image. The figure-3(b) shows the stego/watermarked image of the same size. In the same way, Figure-4(a) shows the Baboon cover image of 1024x1024-pixels size in which message is to be embedded. The figure-4(b) shows the stego/watermarked image. The message/watermark images are shown in figure 3(c) and 4(c) while after extraction the resultant message/watermark images are shown in figure 3(d) and 4(d).

The analysis of the results stated that the input images and resultant images figure 3(a), figure 4(a) and figure 3(b), figure 4(b) respectively are visibly similar. In the same manner, the embedded message/watermark images, shown in figure 3(c), 4(c) are identical with extracted message/watermark images, shown in figure 3(d) and 4(d) respectively in reference to Human Visual System (HVS)[16].

(a)

(b)

(c)

(d)

Figure 3. (a) Lena Original or Cover Image of 512 x 512 pixels before embedment
(b) Stego/Watermarked Image of 512 x 512 pixels after Embedment
(c) Message/Watermark Image of 64 x 64 pixels before embedment
(d) Message/Watermark Image of 64 x 64 pixels after extraction

(a)

(b)

(c)

(d)

Figure 4. (a) Baboon Original or Cover Image of 1024 x 1024 pixels before embedment
(b) Stego/Watermarked Image of 1024 x 1024 pixels after embedment
(c) Message/Watermark Image of 64 x 64 pixels before embedment
(d) Message/Watermark Image of 64 x 64 pixels after extraction

The researchers have also measured image quality of stego/watermarked images while implementing Matrix Transformation Encryption and Embedment Algorithm by observing Peak Signal-to-Noise Ratio (PSNR) value, as shown in table 1 and the extracted message/watermarks' PSNR value as shown in Table 2.

Table I. Stego/Watermarked image's Peak Signal-to-Noise Ratio

Images	Cover/Watermarked Image Pixel Size	Cover/Watermarked Image PSNR (in dB) Value
Lena	512 x 512	77.03
Baboon	1024 x 1024	83.05

Table II. Extracted message/watermark image's Peak Signal-to-Noise Ratio

Stego/ Cover Images	Message Image Pixel Size	Extracted Message/Watermark PSNR (in dB) Value
Lena	64 x 64	Infinite
Baboon	64 x 64	Infinite

V. CONCLUSION

In a comparison of the algorithm, MP_1[16], this work focuses on up to three channels. That means all three channels can be used to embed information. The watermarked or stego images having good PSNR values[17]. The proposed algorithm embedded hiding information scattered through one or more channels of images that makes more complex to detect the secret message. This enhances the robustness[18] of the digital watermark or message. It was also observed that the extracted message/watermark image has highest PSNR value i.e. infinite in both the experimental results shown in Table 2. It is suggested that the message or watermark image size must be less than 256 x 256 pixels.It is also observed that the size of cover/targeted image should be of two times larger than message or watermark image.

VI. ACKNOWLEDGMENT

We are grateful to Dr. N. N. Jani (Ex. Dean Department of Computer Science, KSV Gandhinagar) for providing relentless guidance for the research work. We are also thankful to the cited researchers for their published research work.

VII. REFERENCES

[1] C. Cruz, J. A. Mendoza, M. N. Miyatake, H. P. Meana, and B. Kurkoski, “Semi-fragile watermarking based image authentication with recovery capability,” Proc. - 2009 Int. Conf. Inf. Eng. Comput. Sci. ICIECS 2009, pp. 0–3, 2009.

[2] A. Najafi, A. Siahkoohi, and M. B. Shamsollahi, A content-based digital image watermarking algorithm robust against JPEG compression. IEEE, 2011, pp. 432–437.

[3] S. Alam, V. Kumar, W. a. Siddiqui, and M. Ahmad, “Key Dependent Image Steganography Using Edge Detection Shahzad,” 2014 Fourth Int. Conf. Adv. Comput. Commun. Technol. IEEE, pp. 85–88, 2014.

[4] X. Li, Y. Chen, F. Wang, and T. Qinqin, “The Secret Image Sharing Scheme Based On Improved LSB Algorithm,” ICCCNT - 2014 IEEE, 2014.

[5] K. Mahanta, D. J. Das, H. M. K. R. Bhuyan, A. Dutta, and M. Gogoi, “Design and implementation of an MSI number based image watermarking architecture in the transform domain,2014 IEEE,” Int. Conf. Signal Process. Integr. Networks Des. IEEE, pp. 157–163, 2014.

[6] M. T. Mirza, Q. Ahmed, S. Munib, A. Khan, and R. K. Khalil, “A New Hybrid Domain Based Print-Scan Resilient Image Watermarking Technique,” Proc. - 12th Int. Conf. Front. Inf. Technol. FIT 2014 IEEE, pp. 170–175, 2014.

[7] A. Noel and J. Raj, “Comparison of LSB Based and HS Based Reversible Data Hiding Techniques,” Devices, Circuits Syst. IEEE, no. 978–1–4799–1356–5/14, pp. 5–8, 2014.

[8] N. Sruthi, A. V. Sheetal, and V. Elamaran, “Spatial and spectral digital watermarking with robustness evaluation,” 2014 Int. Conf. Comput. Power, Energy, Inf. Commun. ICCPEIC 2014 IEEE, pp. 500–505, 2014.

[9] E. Dagar and S. Dagar, “LSB based image steganography using X-Box mapping,” Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014, IEEE, pp. 351–355, 2014.

[10] D. Rawat, M. Dc, V. Bhandari, and A. Professor, “A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image,” Int. J. Comput. Appl., vol. 64, no. 20, pp. 975–8887, 2013.

[11] A. Babu, “A Reversible Crypto-Watermarking System for Secure Medical Image Transmission,” 978-1-4673-6540-6/15 IEEE, pp. 1–6, 2015.

[12] E. Bash, “A Lossless Data Hiding Method Based On Inverted LSB Technique,” Image Infonnation Process. A - IEEE, vol. 1, pp. 1–18, 2015.

[13] S. Bhatt, A. Ray, A. Ghosh, and A. Ray, “Image steganography and visible watermarking using LSB extraction technique,” Proc. 2015 IEEE 9th Int. Conf. Intell. Syst. Control. ISCO 2015, 2015.

[14] H. T. Chan, W. J. Hwang, and C. J. Cheng, “Digital hologram authentication using a Hadamard-based reversible fragile watermarking algorithm,” IEEE/OSA J. Disp. Technol., vol. 11, no. 2, pp. 193–203, 2015.

[15] G. S. Charan, S. S. V Nithin Kumar, B. Karthikeyan, V. Vaithiyanathan, and K. Divya Lakshmi, “A novel LSB based image steganography with multi-level encryption,” International Conf. Innov. Information, Embed. Commun. Syst. , IEEE, pp. 1–5, 2015.

[16] M. Pandya and A. Jani, “A Hybrid Approach for Secure Message Communication and Color Image Watermarking,” Elixir Int. J. Digit. Process., vol. 1, no. 114, p. 4, 2018.

[17] A. Singh and H. Singh, “An improved LSB based image steganography technique for RGB images,” Proc. 2015 IEEE Int. Conf. Electr. Comput. Commun. Technol. ICECCT , IEEE, pp. 1–4, 2015.

[18] K. W. K. Wu, W. Y. W. Yan, and J. D. J. Du, A Robust Dual Digital-Image Watermarking Technique. 2007.

[19] Weisstein, Eric W. "Transpose." From MathWorld -- A Wolfram http://mathworld.wolfram.com/Transpose.html

